PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-045507
(43)Date of publication of application : 16.02.1999

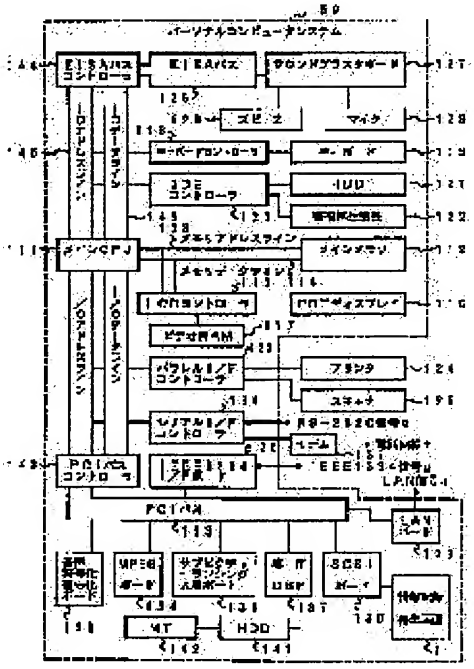
(51)Int.Cl. G11B 20/10
G06F 12/14
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 09-198638
(22)Date of filing : 24.07.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : ANDO HIDEO
NAKAGAWA MASAKI
KOJIMA TADASHI
ISHIZAWA YOSHIYUKI

(54) INFORMATION REPRODUCING DEVICE, RECOGNITION DEVICE, AND INFORMATION PROCESSING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To perform data transmission between a reproducing device and a processing board and to reduce the load on a main control part, by discriminating the kind of reproduced information and setting certification on a specified object to be certified based on the discriminating result.
SOLUTION: At the time of reproducing information, various kinds of streams of information are separated and extracted from a program stream, and are transferred without intervention of a main CPU 111 and directly through a PCI bus 133 to a sound coding and decoding board 136, an MPG board 134 and a board 135 for sub-picture-run-length by an information recording and reproducing device 1. Similarly to the information recording and reproducing device 1, each individual separated and extracted stream is also transferred via an I/O data line 146 and the PCI bus 133 without intervention of the main CPU 111 to the boards 134 and 135 and an SCSI board 136, by the information reproducing device 122. Thus, without intervention of the main CPU 111, data can be transferred between the information recording and reproducing device and also the information reproducing device 122 and the individual boards 134, 135 and 136 respectively, thus reducing the load on the CPU 111.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－45507

(43)公開日　平成11年(1999)２月16日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｄ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｇ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
9/32			６０１Ｅ

審査請求　未請求　請求項の数28　ＯＬ　（全 33 頁）　最終頁に続く

(21)出願番号　特願平9－198638

(22)出願日　平成９年(1997)７月24日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　安東　秀夫
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　中河　正樹
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　小島　正
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

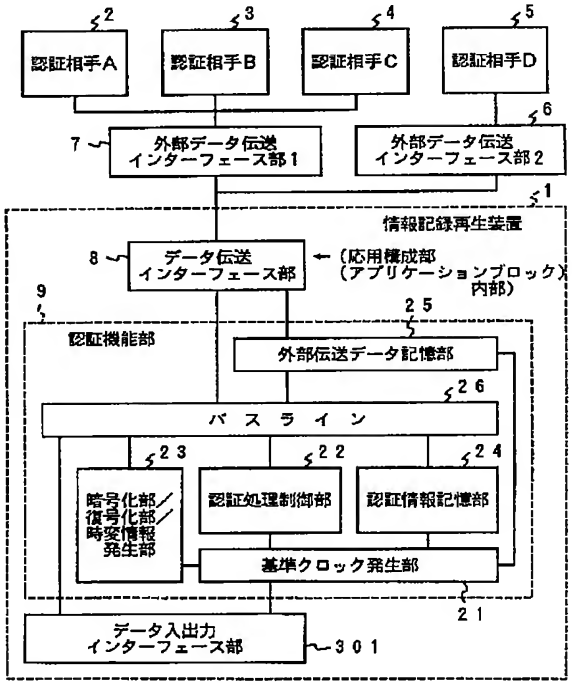
最終頁に続く

(54)【発明の名称】　情報再生装置、認識装置、情報処理システム

(57)【要約】

【課題】　この発明は、メインの制御部が介在せずに、情報記録再生装置と各処理ボードとの情報の伝送を行えることができ、メインＣＰＵの負担を軽減でき、情報伝送期間中にメインＣＰＵが他の処理を行うことができる。

【解決手段】　この発明は、情報記録再生装置１が認証機能を持ち、メインＣＰＵ１１１を介さずに直接、ＭＰＥＧボード１３４、サブピクチャーランレングス用ボード１３５、音声符号化復号化ボード１３６に情報を伝送するようにしたものである。



1

【特許請求の範囲】

【請求項１】　情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報再生装置以外の特定の認証相手に対して認証を行う認証手段と、
を具備したことを特徴とする情報再生装置。

【請求項２】　上記認証手段が、上記認証相手と独自に相互認証と共通の暗号鍵の伝送を行い、かつ上記認証相手との間で上記共通の暗号鍵を利用した暗号化情報を伝送することを特徴とする請求項１に記載の情報再生装置。

【請求項３】　上記認証手段が、上記共通の暗号鍵を用いて情報を暗号化する暗号化部、あるいは暗号化された情報を復号化する復号化部を有することを特徴とする請求項２に記載の情報再生装置。

【請求項４】　上記共通の暗号鍵が、１４ビット以上のサイズを有することを特徴とする請求項２に記載の情報再生装置。

【請求項５】　上記暗号化部、あるいは上記復号化部が、ランダム信号発生器を有し、このランダム信号発生器からのランダム信号を用いて暗号化あるいは復号化を行うことを特徴とする請求項３に記載の情報再生装置。

【請求項６】　上記認証手段が、暗号鍵を発生する発生手段を有し、上記認証相手に対して少なくとも上記暗号鍵を伝送して共有化することを特徴とする請求項１に記載の情報再生装置。

【請求項７】　上記暗号鍵が、１４ビット以上のサイズを有することを特徴とする請求項６に記載の情報再生装置。

【請求項８】　上記認証手段が、時変情報を発生する発生手段を有し、この発生手段からの時変情報を用いて暗号化あるいは復号化を行うことを特徴とする請求項３に記載の情報再生装置。

【請求項９】　上記発生手段が、ランダム信号発生器で構成されることを特徴とする請求項８に記載の情報再生装置。

【請求項１０】　上記認証手段が、第１の暗号鍵を発生させる発生手段と、上記認証相手から送られた第２の暗号鍵を用いて上記第１の暗号鍵を暗号化する暗号化手段と、この暗号化手段により暗号化された上記第１の暗号鍵を上記認証相手に伝送する伝送手段とを有することを特徴とする請求項１に記載の情報再生装置。

【請求項１１】　上記認証手段が、上記発生手段により発生された第１の暗号鍵、上記認証相手から送られた第２の暗号鍵の少なくともいずれかを記憶する記憶手段を有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１２】　情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報記録媒体から再生した情報の種類を判別する判

2

別手段と、
この判別手段の判別結果に基づいて複数の認証相手の１つを認証相手と設定する設定手段と、
を具備したことを特徴とする情報再生装置。

【請求項１３】　上記情報記録媒体に記録されている情報が、少なくとも複数のパケットの集合体として記録され、上記判別手段が少なくともパケット内に記録して有る情報に基付き認証相手を判別することを特徴とする請求項１２に記載の情報再生装置。

【請求項１４】　上記設定手段が、複数の認証相手の候補に対し、伝送したい情報の種類を知らせることにより、該当する認証相手を設定することを特徴とする請求項１２に記載の情報再生装置。

【請求項１５】　上記認証手段が、上記認証相手に伝送する情報を記憶する記憶手段を有することを特徴とする請求項１に記載の情報再生装置。

【請求項１６】　上記認証手段が、独自に基準クロックを発生する発生手段を有し、この発生手段からの基準クロックに基づいて認証を行うことを特徴とする請求項１５に記載の情報再生装置。

【請求項１７】　上記認証手段が、上記認証相手との間で事前に共有化され、上記第２の暗号鍵を暗号化あるいは復号化するための第３の暗号鍵をあらかじめ記憶する記憶手段を有し、この記憶手段に記憶されている第３の暗号鍵を用いて上記第２の暗号鍵を暗号化あるいは復号化する手段とを有することを特徴とする請求項１０に記載の情報再生装置。

【請求項１８】　情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報再生装置以外の特定の認証相手に対して情報の伝送を行う通信手段と、
この通信手段を用いて上記認証相手に対して認証を行う認証手段と、
を具備したことを特徴とする情報再生装置。

【請求項１９】　上記認証手段が、上記認証相手と独自に相互認証と共通の暗号鍵の伝送を上記通信手段を用いて行い、かつ上記認証相手との間で上記共通の暗号鍵を利用した暗号化情報を上記通信手段を用いて伝送することを特徴とする請求項１に記載の情報再生装置。

【請求項２０】　認証処理を行う認証処理制御部と認証処理の内容を記憶する認証情報記憶部とを具備し、
上記認証処理制御部による認証処理の履歴を上記認証情報記憶部に逐次記憶することにより、複数の認証相手との間の並行認識処理を可能とすることを特徴とする認証装置。

【請求項２１】　複数の認証相手から個々に第１の暗号鍵を受け取る受け取り手段と、
複数の認証相手に対して個々の第２の暗号鍵を発行する発行手段と、
上記認証相手から受け取った第１の暗号鍵と認証相手に

対して発行した第２の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成する作成手段と、
複数の認証相手に対して別々に上記各手段に対する処理の履歴を記憶する記憶手段と、
を具備したことを特徴とする認証装置。
【請求項２２】　上記発行手段が、時変情報を発生する発生手段を有し、この発生手段により発生される時変情報を用いて複数の認証相手に対して異なる第２の暗号鍵を発行することを特徴とする請求項２１に記載の認証装置。
【請求項２３】　複数の認証相手から個々に第１の暗号鍵を受け取るステップと、
複数の認証相手に対して個々の第２の暗号鍵を発行するステップと、
上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成するステップとを有し、
複数の認証相手に対して別々に上記各ステップに対する処理の履歴を逐次記憶し、この記憶されている処理の履歴により、複数の認証処理を並行して実行することを特徴とする認証装置。
【請求項２４】　少なくとも暗号鍵の発行とこの発行される暗号鍵に基づいた情報の暗号化と上記発行される暗号鍵に基づいた情報の復号化を行う認識装置において、
上記暗号鍵の発行、情報の暗号化、情報の復号化を行う際に用いるランダム信号を発生する発生手段を具備していることを特徴とする認証装置。
【請求項２５】　認証相手からの第１の暗号鍵を受け取る受け取り手段と、
認証相手に対する第２の暗号鍵を発行する発行手段と、
上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて認証相手との間で共通の第３の暗号鍵を作成する作成手段と、
情報を上記第３の暗号鍵を用いて暗号化する暗号化手段と、
暗号化されている情報を上記第３の暗号鍵を用いて復号化する復号化手段とを具備し、
上記作成手段、暗号化手段、復号化手段が１つの回路で構成されることを特徴とする認証装置。
【請求項２６】　情報を再生する情報再生装置と、この情報再生装置により再生される情報を処理する情報処理回路と、上記情報再生装置と上記情報処理回路を制御するメインＣＰＵとからなる情報処理システムにおいて、
上記メインＣＰＵを介在せずに、上記情報再生装置と上記情報処理回路との間で相互認証を行うことを特徴とする情報処理システム。
【請求項２７】　第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムにおいて、
上記第１の装置が、
識別用の情報を出力する第１の出力手段と、
この第１の出力手段に応答して上記第２の装置から供給される第１の暗号化キーに基づいて、あらかじめ記憶されている第２の暗号化キーを暗号化する第１の暗号化手段と、
上記識別用の情報に基づいて第３の暗号化キーを作成する第１の作成手段と、
上記第１の暗号化手段により暗号化された第２の暗号化キーと、上記第１の作成手段により作成された第３の暗号化キーとを出力する第２の出力手段と、
この第２の出力手段に応答して上記第２の装置から供給される暗号化されている第４の暗号化キーを上記作成手段により作成された第３の暗号化キーを用いて復号化する第１の復号化手段と、
この第１の復号化手段により復号化された第４の暗号化キーと上記第２の暗号化キーとに基づいて共通鍵を生成する第１の生成手段と、
この第１の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第１の処理手段とからなり、
上記第２の装置が、
上記第１の装置から供給される上記識別用の情報に基づいて第１の暗号化キーを作成する第２の作成手段と、
この第２の作成手段により作成された第１の暗号化キーとを出力する第３の出力手段と、
この第３の出力手段に応答して上記第１の装置から供給される第３の暗号化キーに基づいて、あらかじめ記憶されている第４の暗号化キーを暗号化する第２の暗号化手段と、
この第２の暗号化手段により暗号化された第４の暗号化キーを出力する第４の出力手段と、
上記第３の出力手段に応答して上記第１の装置から供給される第２の暗号化キーを上記第２の作成手段により作成された第１の暗号化キーを用いて復号化する第２の復号化手段と、
この第２の復号化手段により復号化された第２の暗号化キーと上記第４の暗号化キーとに基づいて共通鍵を生成する第２の生成手段と、
この第２の生成手段により生成された共通鍵を用いて情報の符号化、復号化を第２の処理手段とからなることを特徴とする情報処理システム。
【請求項２８】　第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムにおいて、
上記第１の装置が、
ＡＧＩＤ、設定エリア情報、ストリームＩＤからなる識別用の情報を出力する第１の出力手段と、
時変情報に基づいて第１の暗号化キーを生成する第１の生成手段と、
上記第１の出力手段に応答して上記第２の装置から供給される暗号化されている第１のチャレンジキーを上記識

別用の情報からなる合成キーに基づいて復号化する第１の復号化手段と、
この第１の復号化手段により復号化された第１のチャレンジキーに基づいて、上記第１の生成手段により生成される第１の暗号化キーを暗号化する第１の暗号化手段と、
時変情報に基づいて第２のチャレンジキーを生成する第２の生成手段と、
上記識別用の情報からなる合成キーに基づいて、上記第２の生成手段により生成される第２のチャレンジキーを暗号化する第２の暗号化手段と、
上記第１の暗号化手段により暗号化された第１の暗号化キーと、上記第２の暗号化手段により暗号化された第２のチャレンジキーとを出力する第２の出力手段と、
この第２の出力手段に応答して上記第２の装置から供給される暗号化されている第２の暗号化キーを上記第２の生成手段により生成された第２のチャレンジキーを用いて復号化する第２の復号化手段と、
この第２の復号化手段により復号化された第２の暗号化キーと上記第１の生成手段により生成される第１の暗号化キーとに基づいて共通鍵を生成する第３の生成手段と、
この第３の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第１の処理手段とからなり、
上記第２の装置が、
上記第１の装置から供給される上記識別用の情報に基づいて第１のチャレンジキーを生成する第４の生成手段と、
この第４の生成手段により生成された第１のチャレンジキーとを出力する第３の出力手段と、
この第３の出力手段に応答して上記第１の装置から供給される暗号化されている第２のチャレンジキーを、上記第１の装置から供給される上記識別用の情報からなる合成キーに基づいて、復号化する第３の復号化手段と、
時変情報に基づいて第２の暗号化キーを生成する第５の生成手段と、
上記第３の復号化手段により復号化された第２のチャレンジキーに基づいて、上記第５の生成手段により生成される第２の暗号化キーを暗号化する第３の暗号化手段と、
この第３の暗号化手段により暗号化された第２の暗号化キーを出力する第４の出力手段と、
上記第３の出力手段に応答して上記第１の装置から供給される暗号化されている第１の暗号化キーを上記第４の生成手段により生成された第１のチャレンジキーを用いて復号化する第４の復号化手段と、
この第４の復号化手段により復号化された第１の暗号化キーと上記第５の生成手段により生成される第２の暗号化キーとに基づいて共通鍵を生成する第６の生成手段と、

この第６の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第２の処理手段とからなることを特徴とする情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、情報記録媒体に記録されている情報を再生する情報再生装置、認証処理を行う認証装置、第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムに関する。

【０００２】

【従来の技術】従来、ＤＶＤ等の光ディスクに記録されている映像情報、音声情報、静止画情報など混在する情報を光ディスク装置により再生するものが実用化されている。このような光ディスク装置により再生された情報はその情報の種類に応じて異なった処理回路により処理されるようになっている。

【０００３】たとえば、情報としてＭＰＥＧビデオデータ、オーディオデータ（ＰＣＭ、ＡＣ３）、サブピクチャーデータ、ナビゲーションデータ等からなる場合に、それぞれのデータに合わせた処理ボードにより処理が行われるようになっている。

【０００４】この場合、メインの制御部が、一旦それらのデータを取り込み、この取り込んだデータに応じて各処理ボードにデータを配送していた。

【０００５】この場合、そのデータ配送の期間中、メインの制御部が占有されてしまうので、光ディスク装置から再生する情報量が多くなるとメインの制御部の負担が増え、長時間メインの制御部が他の処理を行うことができなくなるという問題がある。

【０００６】また、従来、暗号化技術として知られている双方向本人認証方法はＲＳＡ（公開鍵暗号のアルゴリズム）のような公開鍵（アシンメトリックキー）を用いた電子署名を用いた方法が良く知られている。

【０００７】たとえば、その方法は

1〕“チャレンジ”としてＡがＢにランダムな文字を送信する。

【０００８】2〕“レポート”としてＢはその文字をＢが持っている公開鍵でサインしてＡへ返送する。ＡはＢが持っている公開鍵を保管している第３者である認証局（ＣＡセンタ）に問い合わせてＢから返送された情報を復号化（解読）する。解読結果がＡが最初に送信した文字と一致すればＢが本人と認める。

【０００９】3〕“チャレンジ”としてＢがＡにランダムな文字を送信する。

【００１０】4〕“レポート”としてＡはその文字をＡが持っている公開鍵でサインしてＢへ返送する。ＢはＡが持っている公開鍵を保管している第３者である認証局（ＣＡセンタ）に問い合わせてＢから返送された情報を復号化（解読）する。解読結果がＢが最初に送信した文

字と一致すればＡが本人と認める。
【００１１】が知られている。
【００１２】しかしこの方法では公開鍵を保管している第３者（認証局（ＣＡセンタ））を必要とし、しかも双方向本人認証毎に通信で公開鍵を保管している第３者である認証局（ＣＡセンタ）に問い合わせる必要があり、処理が非常に煩雑となるという問題がある。
【００１３】さらに、第３者が管理する公開鍵を使用する場合には公開鍵が盗まれやすく、セキュリティ保護が難しかった。
【００１４】また、相互に暗号鍵を交換し合う方法は従来知られていたが、伝送すべき情報をその暗号鍵で暗号化する以外は、相互に交換し合った暗号鍵の使い方については余り知られて無い。
【００１５】さらに、上記の方法では、認証すべき相手の居場所が事前に分かっており、ある送信したい情報が決まっていて、送信すべき相手を探したい場合には上記の方法は意味をなさない。このように従来は認証したい相手を探す方法に付いて有効な方法が無かった。
【００１６】
【発明が解決しようとする課題】この発明は、メインの制御部が介在せずに、情報再生装置と各処理ボードとのデータの伝送を行えることができ、メインの制御部の負担を軽減でき、情報伝送期間中にメインの制御部が他の処理を行うことができる。
【００１７】また、この発明は、非常に簡単な構成で暗号化／復号化（解読）を行える。
【００１８】また、この発明は、公開鍵を管理する第３者を置くことなく容易に相互認証可能、つまり第３者の介在や第３者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。
【００１９】また、この発明は、伝送し合った暗号鍵で他方の暗号鍵を更に暗号化することにより、公開鍵方式を用いるよりも遙かに暗号化の信頼性が高く、情報漏洩を防げる。
【００２０】また、この発明は、情報記録媒体からの情報に付与されている情報の種類を示す情報（ストリームＩＤ）から認証相手を同定することにより、各認証相手に対して認証後、各認証相手にパラレルに情報を配信（送信）でき、この結果、各認証相手の負担が相対的に軽減すると共に情報記録媒体から情報再生を開始してから短時間で画面上に表示でき、タイムラグを最小に抑えることができる。
【００２１】また、この発明によれば、送信したい情報から認証相手を探すことができ、認証候補相手に対して情報を提供し、該当相手から回答してもらい、その回答結果に基付き相互認証作業に入るという方式により、比較的簡単な方法で認証相手を探すことができる。
【００２２】
【課題を解決するための手段】この発明の情報再生装置は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報再生装置以外の特定の認証相手に対して認証を行う認証手段からなる。
【００２３】この発明の情報再生装置は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報記録媒体から再生した情報の種類を判別する判別手段、およびこの判別手段の判別結果に基づいて複数の認証相手の１つを認証相手と設定する設定手段からなる。
【００２４】この発明の情報再生装置は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報再生装置以外の特定の認証相手に対して情報の伝送を行う通信手段、およびこの通信手段を用いて上記認証相手に対して認証を行う認証手段からなる。
【００２５】この発明の認証装置は、認証処理を行う認証処理制御部と認証処理の内容を記憶する認証情報記憶部とを具備し、上記認証処理制御部による認証処理の履歴を上記認証情報記憶部に逐次記憶することにより、複数の認証相手との間の並行認識処理を可能とする。
【００２６】この発明の認証装置は、複数の認証相手から個々に第１の暗号鍵を受け取る受け取り手段、複数の認証相手に対して個々の第２の暗号鍵を発行する発行手段、上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成する作成手段、および複数の認証相手に対して別々に上記各手段に対する処理の履歴を記憶する記憶手段からなる。
【００２７】この発明の認証装置は、複数の認証相手から個々に第１の暗号鍵を受け取るステップと、複数の認証相手に対して個々の第２の暗号鍵を発行するステップと、上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成するステップとを有し、複数の認証相手に対して別々に上記各ステップに対する処理の履歴を逐次記憶し、この記憶されている処理の履歴により、複数の認証処理を並行して実行するものである。
【００２８】この発明の認証装置は、少なくとも暗号鍵の発行とこの発行される暗号鍵に基づいた情報の暗号化と上記発行される暗号鍵に基づいた情報の復号化を行うものにおいて、上記暗号鍵の発行、情報の暗号化、情報の復号化を行う際に用いるランダム信号を発生する発生手段からなる。
【００２９】この発明の認証装置は、認証相手からの第１の暗号鍵を受け取る受け取り手段、認証相手に対する第２の暗号鍵を発行する発行手段、上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて認証相手との間で共通の第３の暗号鍵を作成する作成手段、情報を上記第３の暗号鍵を用いて暗号化する暗号化手段、および暗号化されている情報を上記第３の暗号鍵を用いて復号化する復号化手段からな

り、上記作成手段、暗号化手段、復号化手段が１つの回路で構成される。

【００３０】この発明の情報処理システムは、情報を再生する情報再生装置と、この情報再生装置により再生される情報を処理する情報処理回路と、上記情報再生装置と上記情報処理回路を制御するメインＣＰＵとからなるものにおいて、上記メインＣＰＵを介在せずに、上記情報再生装置と上記情報処理回路との間で相互認証を行う。

【００３１】この発明の情報処理システムは、第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行うものにおいて、上記第１の装置が、識別用の情報を出力する第１の出力手段と、この第１の出力手段に応答して上記第２の装置から供給される第１の暗号化キーに基づいて、あらかじめ記憶されている第２の暗号化キーを暗号化する第１の暗号化手段と、上記識別用の情報に基づいて第３の暗号化キーを作成する第１の作成手段と、上記第１の暗号化手段により暗号化された第２の暗号化キーと、上記第１の作成手段により作成された第３の暗号化キーとを出力する第２の出力手段と、この第２の出力手段に応答して上記第２の装置から供給される暗号化されている第４の暗号化キーを上記作成手段により作成された第３の暗号化キーを用いて復号化する第１の復号化手段と、この第１の復号化手段により復号化された第４の暗号化キーと上記第２の暗号化キーとに基づいて共通鍵を生成する第１の生成手段と、この第１の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第１の処理手段とからなり、上記第２の装置が、上記第１の装置から供給される上記識別用の情報に基づいて第１の暗号化キーを作成する第２の作成手段と、この第２の作成手段により作成された第１の暗号化キーとを出力する第３の出力手段と、この第３の出力手段に応答して上記第１の装置から供給される第３の暗号化キーに基づいて、あらかじめ記憶されている第４の暗号化キーを暗号化する第２の暗号化手段と、この第２の暗号化手段により暗号化された第４の暗号化キーを出力する第４の出力手段と、上記第３の出力手段に応答して上記第１の装置から供給される第２の暗号化キーを上記第２の作成手段により作成された第１の暗号化キーを用いて復号化する第２の復号化手段と、この第２の復号化手段により復号化された第２の暗号化キーと上記第４の暗号化キーとに基づいて共通鍵を生成する第２の生成手段と、この第２の生成手段により生成された共通鍵を用いて情報の符号化、復号化を第２の処理手段とからなる。

【００３２】この発明の情報処理システムは、第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行うものにおいて、上記第１の装置が、ＡＧＩＤ、設定エリア情報、ストリームＩＤからなる識別用の情報を出力する第１の出力手段と、時変情報に基づいて第１の暗号化キーを生成する第１の生成手段と、上記第１の出力手段に応答して上記第２の装置から供給される暗号化されている第１のチャレンジキーを上記識別用の情報からなる合成キーに基づいて復号化する第１の復号化手段と、この第１の復号化手段により復号化された第１のチャレンジキーに基づいて、上記第１の生成手段により生成される第１の暗号化キーを暗号化する第１の暗号化手段と、時変情報に基づいて第２のチャレンジキーを生成する第２の生成手段と、上記識別用の情報からなる合成キーに基づいて、上記第２の生成手段により生成される第２のチャレンジキーを暗号化する第２の暗号化手段と、上記第１の暗号化手段により暗号化された第１の暗号化キーと、上記第２の暗号化手段により暗号化された第２のチャレンジキーとを出力する第２の出力手段と、この第２の出力手段に応答して上記第２の装置から供給される暗号化されている第２の暗号化キーを上記第２の生成手段により生成された第２のチャレンジキーを用いて復号化する第２の復号化手段と、この第２の復号化手段により復号化された第２の暗号化キーと上記第１の生成手段により生成される第１の暗号化キーとに基づいて共通鍵を生成する第３の生成手段と、この第３の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第１の処理手段とからなり、上記第２の装置が、上記第１の装置から供給される上記識別用の情報に基づいて第１のチャレンジキーを生成する第４の生成手段と、この第４の生成手段により生成された第１のチャレンジキーとを出力する第３の出力手段と、この第３の出力手段に応答して上記第１の装置から供給される暗号化されている第２のチャレンジキーを、上記第１の装置から供給される上記識別用の情報からなる合成キーに基づいて、復号化する第３の復号化手段と、時変情報に基づいて第２の暗号化キーを生成する第５の生成手段と、上記第３の復号化手段により復号化された第２のチャレンジキーに基づいて、上記第５の生成手段により生成される第２の暗号化キーを暗号化する第３の暗号化手段と、この第３の暗号化手段により暗号化された第２の暗号化キーを出力する第４の出力手段と、上記第３の出力手段に応答して上記第１の装置から供給される暗号化されている第１の暗号化キーを上記第４の生成手段により生成された第１のチャレンジキーを用いて復号化する第４の復号化手段と、この第４の復号化手段により復号化された第１の暗号化キーと上記第５の生成手段により生成される第２の暗号化キーとに基づいて共通鍵を生成する第６の生成手段と、この第６の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第２の処理手段とからなる。

【００３３】

【発明の実施の形態】以下、図面を参照してこの発明の実施の形態に係る情報記録再生装置を説明する。

【００３４】図１に認証機能を有する情報記録再生装置

の構成説明図を示す。

【００３５】すなわち、情報記録再生装置１は情報記録媒体（光ディスク）２０１から情報を再生もしくは情報の記録を行う情報記録再生部（物理系ブロック）２００、認証機能部９、通信機能部３０１、コンピュータ接続インターフェース部３０２、情報記録再生装置１内全体の制御を行う制御部３０３、および各部を接続するバスライン２６から構成されている。

【００３６】情報記録再生装置１は通信機能部３０１を有することによりネットワークを介して独自に情報を伝送できる。特にネットワークサーバの記録装置として使うため、各種の通信機能を持っている。一般にはＬＡＮ接続Ｉ／Ｆ部３０４を経由して各クライアントに情報の伝送を行う。それに限らず電話回線を使い、ＬＡＮに直接接続してないクライアントや携帯端末との間の情報伝送も可能になっている。電話回線で伝送する場合、電話番号を指定するためのＮＣＵ部３０５とＮＣＵ部３０６を持つ。アナログ信号で伝送を希望するクライアントまたは携帯端末に対してはモデムＩ／Ｆ部３０７を介して情報の伝送を行い、ディジタル信号での伝送を希望するクライアントまたは携帯端末に対してはＩＳＤＮＩ／Ｆ部３０８から情報の伝送を行う。更にＰＨＳ機能を内蔵した情報携帯端末との間の情報交換はＰＨＳＩ／Ｆ部３０９を利用する。

【００３７】図２～図６を用いて情報記録再生装置１内にある認証機能部９の内部構造説明と機能説明を行う。

【００３８】［１］認証機能の概要説明（認証機能とは何か）

［１－１］情報記録再生装置と外部接続相手との間の関係

図２に認証機能部の内部構造とそれに接続される周辺機器との関係を示す。

【００３９】上記情報記録媒体２０１から再生された情報もしくは情報記録媒体２０１へ記録される情報は情報記録再生装置１内のデータ伝送インターフェース部８を介して外部接続相手との間で伝送される。

【００４０】情報伝送相手となる外部接続相手は複数存在し、例えば図２のように認証相手Ａ：２、認証相手Ｂ：３、認証相手Ｃ：４、認証相手Ｄ：５などが接続されている。

【００４１】外部接続相手との間の情報伝送を行った場合、例えば外部データ伝送インターフェース部２：６を経て認証相手Ｄ：５に接続されたり、外部データ伝送インターフェース部１：７が各認証相手Ａ：２、Ｂ：３、Ｃ：４へ情報を配送する。

【００４２】［１－２］複数の外部接続相手との間の情報伝送方法

図２のように情報記録再生装置１が複数の接続相手とつながり、

１）情報記録媒体２０１に記録するあるいは情報記録媒体２０１から再生する情報の内容に応じて特定の外部接続相手のみとの情報伝送を行う

２）複数の異なる内容の情報に応じて同時に複数の外部接続相手とそれぞれ独自に情報伝送を行う

３）特定の外部接続相手との間で伝送した情報は他の外部接続相手が傍受不可能と言う操作を実行するため

◎外部接続相手との間で情報を暗号化して伝送する

◎暗号化した情報伝送に先立ち、各外部接続相手毎に暗号化用の鍵を共有するを行っている。

【００４３】［１－３］複数の外部接続相手との事前の認証作業

外部接続相手との間で暗号化した情報を伝送する前に、事前の認証作業を行う。

【００４４】１）情報記録媒体２０１に記録するあるいは情報記録媒体２０１から再生する情報の内容に応じて適合した外部接続相手（認証相手）を捜す

２）捜し当てた認証相手（外部接続相手）毎にＩＤ番号を発行する

３）捜し当てた認証相手（外部接続相手）が本物であるかを“チャレンジレスポンス”と言う方法（詳細は後述）を用いて確認する

４）特定の認証相手のみと共有できる秘密の暗号解読鍵を作成すると言う一連の処理により認証作業が行われる。

【００４５】［１－４］ネットワークシステムにおける情報伝送の具体例

上記の概要説明に付いての具体的実施例に従った説明を以下に行う。

【００４６】図２に示した接続をネットワークシステムに適応した場合には、情報記録再生装置１はネットワークサーバのメインメモリドライブとして使われる。ネットワークサーバの分散処理に従って情報記録再生装置１が独自に情報の配送・収集を行う。

【００４７】ネットワークサーバから情報の配送・収集先のクライアント（のＩＰアドレスや電話番号）と配送・収集する情報内容を通知された後は、ネットワークサーバのメインＣＰＵを介さずに情報記録再生装置１が直接クライアントと交信を開始する。

【００４８】従ってネットワークシステムに適応した場合は認証相手Ａ：２、認証相手Ｂ：３、認証相手Ｃ：４、認証相手Ｄ：５は個々のクライアントマシン（ＰＣなど）を意味する。またデータ伝送インターフェース部８は“ＬＡＮ用Ｉ／Ｆ部”もしくは“モデム”や“ＰＨＳなどのデジタル通信用Ｉ／Ｆ部”に対応し、外部データ伝送インターフェース部１：７はネットワーク上の“ファイアーウォール”あるいは“ルーター”“ゲートウェイ”“ブリッジ”などに対応する。１台のクライアントマシン（認証相手Ｄ５）につながる外部データ伝送インターフェース部２：６をクライアントマシン内に内蔵されている“ＬＡＮ用Ｉ／Ｆ部”もしくは“モデム”

や“ＰＨＳなどのデジタル通信用Ｉ／Ｆ部”に対応するとの解釈もできる。

【００４９】上記データ伝送インタフェース部８は、図１に示す通信機能部３０１内のＬＡＮ接続Ｉ／Ｆ部３０４、モデムＩ／Ｆ部３０７、ＩＳＤＮＩ／Ｆ部３０８、ＰＨＳＩ／Ｆ部３０９に対応する。

【００５０】［１－５］ＰＣシステム内での情報伝送の具体例

ＰＣ（パーソナルコンピュータ）システム内での外部接続相手（認証相手）としては以下の２種類の場合が有る

［１－５－１］ＰＣ内の記録装置

外部接続相手（認証相手）としてはＡＴＡＰＩ（ＡＴアタッチメントパケットインターフェース）やＳＣＳＩ（スカジー）、ＩＥＥＥ１３９４（米国電機電子技術者協会企画のシリアルインターフェース）などで接続される“ＨＤＤ”“ＣＤ－ＲＯＭ”“ＭＯ”“ＰＤ（相変化型記録ドライブ）”“ＤＶＤ－ＲＯＭ”“ＤＶＤ－ＲＡＭ”“半導体メモリ”などの記録装置を意味し、データ伝送インターフェース部８、外部データ伝送インターフェース部７、外部データ伝送インターフェース部６はＡＴＡＰＩやＳＣＳＩ、ＩＥＥＥ１３９４などのインターフェース部を示す。

【００５１】［１－５－２］ＰＣ内の信号処理部

外部接続相手（認証相手）としては“ＭＰＥＧエンコード／デコード部”“サウンドブラスタ部”“オーディオ信号圧縮伸長部”“サブピクチャーランレングス用ボード”“プログラム実行用ＣＰＵ”などの信号処理部を意味し、データ伝送インターフェース部８、外部データ伝送インターフェース部７、外部データ伝送インターフェース部６はＡＴＡＰＩやＳＣＳＩ、ＩＥＥＥ１３９４などのインターフェース部を示す。

【００５２】上記情報記録再生装置１としては、たとえば図２に示すデータ伝送インターフェース部８、認証機能部９、データ入出力インターフェース部３０を有する後述する情報記録再生部（物理ブロック）２００（図９参照）により構成されている。

【００５３】上記認証相手も上記認証機能部９と同じ構成のものを有している。認証相手が単体の場合には、後述する認証情報記憶部２４の縦１列の情報が記憶される。

【００５４】［２］情報記録媒体２０１の記録内容と認証相手設定との関係

［２－１］ＤＶＤ-ビデオにおけるフォーマット構造

ＤＶＤ-ビデオの情報は大きくＶＭＧ（ビデオ　マネージャー）とＶＴＳ（ビデオ　タイトル　セット）に分けられる。

【００５５】ＶＭＧ（ビデオ　マネージャー）はメニューあるいはタイトルを再生するための制御情報を含み、ＶＴＳ（ビデオ　タイトル　セット）は映像データを構成する各種エレメントの構成が同じであるタイトルの集まりになっている。

【００５６】ＶＴＳ（ビデオ　タイトル　セット）内の再生用の映像データの集まりをＶＯＢＳ（ビデオ　オブジェクト　セット）と呼ぶ。ＶＯＢＳはＭＰＥＧ２のＰＳ（プログラムストリーム）構造を取るＶＯＢ（ビデオ　オブジェクト）の集まりである。

【００５７】また各ＶＯＢは、制作者の目的に応じたシーン単位にセル（セル）に分割する事が可能である。

【００５８】さらに各セルは複数のＶＯＢＵ（ビデオ　オブジェクト　ユニット）から構成されている。

【００５９】［２－２］ＤＶＤ-ビデオにおける情報記録媒体２０１の記録内容

ＶＯＢＵ内部は“ビデオ情報”“オーディオ情報”“サブピクチャー情報”“ナビゲーション情報”が混在して記録され、それぞれの情報が『パック』と呼ばれるブロック毎のかたまり単位で時分割されて情報記録媒体２０１に記録されている。

【００６０】図３に情報記録媒体２０１に記録されているＶＯＢＵ内部構造説明図を示す。ディスク形状の情報記録媒体２０１では内周から外周に向かってスパイラル状にトラックが連続しており、図３はそのトラックに沿って記録して有る情報の一部を示している。

【００６１】例えば図３の“ａパック１０ａ”がビデオ情報が記録されている“ビデオパック”に対応し、“ｂパック１０ｂ”がオーディオ情報が記録されている“オーディオパック”に対応する。オーディオパックはＡＣ－３またはＰＣＭ形式でオーディオ情報が記録されている。さらに一例として“ｃパック１０ｃ”が字幕や挿入静止画などの情報を持つ“サブピクチャーパック”、“ｄパック１０ｄ”が次のアクセス先などを示す“ナビゲーションパック”に対応する。

【００６２】各パックの集合により形成されるストリームとしては、ビデオデータストリーム、オーディオデータストリーム、サブピクチャーデータストリーム、ナビゲーションデータストリーム、ドルビー／リニアオーディオデータストリーム等からなる。

【００６３】［２－３］ＤＶＤ-ビデオにおける記録内容と認証相手設定との関係

図２に示した情報記録再生装置１がＰＣ（パーソナルコンピュータ）に接続されている場合には“［１－５－２］ＰＣ内の信号処理部”で説明したように各認証相手はＰＣ内に組み込まれている各種信号処理用ボードに対応する。例えば認証相手Ａ：２がＭＰＥＧエンコーダ／デコーダボードを意味し、認証相手Ｂ：３がＡＣ－３またはＰＣＭのデコードボード、あるいはサウンドブラスタボードやＭＰＥＧオーディオのエンコーダ／デコーダボードに対応する。更に例として認証相手Ｃ：４がサブピクチャーランレングス用ボードやキャラクタージェネレーターボードに対応し、認証相手Ｄ：５がＳＣＳＩラインなどを経由してＰＣＩバス、メインＣＰＵのＩ／Ｏ

データラインを経て到達するＰＣのメインＣＰＵに対応させる事ができる。

【００６４】上記情報記録再生装置１に内蔵される認証機能部９では図３に示される情報記録媒体２０１上の記録情報の内、ａパック１０ａのみの情報を切り出して取り出し、認証相手Ａ：２に伝送する。同様に認証機能部９ではｂパック１０ｂ部分を抜き出して認証相手Ｂ：３へ伝送し、ｃパック１０ｃ部分を抜き出して認証相手Ｃ：４へ伝送する。

【００６５】また例えばナビゲーションパックの情報であるｄパック１０ｄ情報を認証相手Ｄ：５であるＰＣのメインＣＰＵが受け取り、その情報に応じて次にアクセスする位置を判断する。

【００６６】［２－４］ＤＶＤ-ビデオにおける情報内容の識別方法

図３に示した各パック内部は、図４に示すようにパックヘッダ１１とパケット１２に分かれている。

【００６７】パックヘッダ１１は４バイトのパックスタートコード、６バイトのシステムクロックリファレンス、３バイトの転送レート表示コードなどから構成されている。

【００６８】パケット１２は更にパケットヘッダ１３と伝達される情報内容１４に分かれる。パケットヘッダ１３内には３バイトのパケットスタートコードや１バイトのストリームＩＤが含まれている。

【００６９】このパケットヘッダ１３内のストリームＩＤに伝送される情報の種類（ストリーム）が記述されている。具体的には

○ストリームＩＤが“１１１００００”の時には伝送される情報内容１４がビデオ情報（ビデオストリーム）を意味し、そのパケット１２を含むパックはビデオパックを構成する。

【００７０】○ストリームＩＤが“１１０Ｘ０＊＊＊”（＊＊＊はデコーディングオーディオストリーム番号）の時には伝送される情報内容１４がＭＰＥＧオーディオに基付くオーディオ情報（オーディオストリーム）を意味し、そのパケット１２を含むパックはオーディオを構成する。

【００７１】○ストリームＩＤが“１０１１１１０１”の時には伝送される情報内容１４がプライベートストリーム１である事を意味し、“ＭＰＥＧオーディオ以外のオーディオ情報”か“サブピクチャー情報”がそれに含まれる。

【００７２】○ストリームＩＤが“１０１１１１１１”の時には伝送される情報内容１４がナビゲーション情報（プライベートストリーム２）を意味し、そのパケット１２を含むパックはナビゲーションパックを構成する。

【００７３】となっている。特にストリームＩＤが“１０１１１１０１”のプライベートストリーム１の場合には、図４の“伝送される情報内容１４”の最初に、詳細な情報の種類を示すサブストリームＩＤ（１バイト）が記録されている。具体的には

○サブストリームＩＤが“００１＊＊＊＊＊”（＊＊＊＊＊はデコーディングサブピクチャー番号）の時には伝送される情報内容１４がサブピクチャー　情報（サブピクチャーストリーム）を意味し、そのパケット１２を含むパックはサブストリームパックを構成する。

【００７４】○サブストリームＩＤが“１００００＊＊＊”（＊＊＊はデコーディングオーディオストリーム番号）の時には伝送される情報内容１４がDolby ＡＣ－３を意味し、そのパケット１２を含むパックはオーディオパックを構成する。

【００７５】○サブストリームＩＤが“１０１００＊＊＊”（＊＊＊はデコーディングオーディオストリーム番号）の時には伝送される情報内容１４がリニアーＰＣＭを意味し、そのパケット１２を含むパックはオーディオパックを構成する。

【００７６】となっている。

【００７７】このように情報記録媒体２０１から再生される情報に対して、図２の認証機能部９で図４のパケット１２内に記録されているストリームＩＤとサブストリームＩＤを読み取り、各パック１０ａ～１０ｄの情報の種類を識別する。

【００７８】［２－５］プログラムソフトにおける記録内容と認証相手設定との関係

ＤＶＤ-ビデオではビデオ情報やオーディオ情報というコンテンツ情報のみが記録されているが、コンピュータシステム上では更にテキスト情報やアプリケーション実行用のソフトプログラムが混在している。ＰＣの分散処理に対応して情報記録再生装置１がＰＣのＣＲＴに表示されている画面を受信したり、同時にＨＤＤやＣＤ－ＲＯＭなどの記録装置からソフトプログラムや音声／ビデオ情報を受信する必要が生じる。

【００７９】特に音声情報やビデオ情報を伝送する場合には途中で途切れないようにする工夫が必要となる。そのためビデオ情報と音声情報やソフトプログラム、テキスト情報を同時に転送する場合にはビデオ情報を細かくブロック毎に区切り、その合間に他の情報を断続的に入れ込む必要がある。従って情報記録再生装置１が外部から各種の情報を受信し、情報記録媒体２０１に記録するにはデータ伝送インターフェース部８に入力される情報は図３のように情報種類毎にパック構造またはパケット構造を持ってブロック化され、時分割されている。

【００８０】ＰＣシステムの場合は受信した情報をファイル形式で情報記録媒体２０１に記録する。各ファイル名には拡張子が付けられ、“.TXT”“.WAV”“.BMP”“.JPEG”“.MPEG”など拡張子（ストリームＩＤの代りになる）により情報種類を識別できる。

【００８１】［２－６］ネットワークシステムにおける記録内容と認証相手設定との関係

ネットワークシステムの場合には伝送情報毎の送信／受信先クライアントマシンのＩＰアドレスやモデムを用いる場合の電話番号をサーバ本体のメインＣＰＵから指示を受ける。図３のように複数情報を時分割して伝送する以外に同一の情報を一度にまとめて伝送する場合もある。

【００８２】［３］認証機能部９内部構造の簡易説明と情報伝送方法

［３－１］認証機能部９内の構成要件

認証機能部９内部の概略構造を図２に示す。認証機能部９は“基準クロック発生部２１”“認証処理制御部２２”“暗号化部／復号化部／時変情報発生部２３”“認証情報記憶部２４”“外部伝送データ記憶部２５”と各部間の情報の入出力を媒介する共通の“バスライン２６”から構成される。

【００８３】［３－２］認証処理制御部２２

認証処理制御部２２では

◎パケット１２内のストリームＩＤ、サブストリームＩＤを読み取り、対応する認証相手２～５の割り出し処理

◎認証相手２～５毎のＩＤ番号の発行処理

◎認証相手２～５との事前の認証作業と認証相手２～５毎の独自の共通暗号鍵（バスキー）の作成処理

◎作成した暗号鍵を用いた情報の暗号化処理

◎作成した暗号鍵を用いた暗号化された情報の復号化処理と言ういっさいの認証関連処理の実行制御を行う。

【００８４】［３－３］認証情報記憶部２４

認証情報記憶部２４は半導体メモリ素子（たとえばＥＥＰＲＯＭ）で構成され、認証関連処理に必要な

◎暗号鍵作成のための必要情報

◎認証相手毎に作成した暗号鍵情報

◎認証相手毎に行う後述する一連の認証手順履歴情報が記録される。

【００８５】［３－４］暗号化部／復号化部／時変情報発生部２３

暗号化部／復号化部／時変情報発生部２３では認証関連処理に必要な

“◎暗号鍵の作成”　“◎暗号化”　“◎復号化”の実行を行う。

【００８６】［３－５］外部伝送データ記憶部２５

各認証相手２～５との間では暗号化された情報の送受信が行われる。この送受信時に使われる暗号化された情報を外部伝送データ記憶部２５に記録している。

【００８７】上記情報記録再生装置１内のデータ入出力インターフェース部３０から出力された情報記録媒体２０１からの再生情報はバスライン２６を経由して暗号化部／復号化部／時変情報発生部２３に入り、そこで暗号化された後、再びバスライン２６を経由して外部伝送データ記憶部２５に保存される。暗号化された情報を外部に伝送する場合はデータ伝送インターフェース部８が直接この外部伝送データ記憶部２５からデータを読み出す。（情報記録媒体２０１からのデータ再生時）

各認証相手２～５から受信した暗号化された情報も、データ伝送インターフェース部８から直接この外部伝送データ記憶部２５に一時的に保存される。この情報を情報記録媒体２０１に記録する場合には暗号化された情報が外部伝送データ記憶部２５からバスライン２６を経由して暗号化部／復号化部／時変情報発生部２３に入る。暗号化部／復号化部／時変情報発生部２３で復号化された後、バスライン２６を経由して情報記録再生部（物理系ブロック）２００内のデータ入出力インターフェース部３０へ送られる。（情報記録媒体２０１へのデータ記録時）

［３－６］基準クロック発生部２１

認証機能部９内では独自のクロックを持って認証関連処理を行っている。この独自のクロックを基準クロック発生部２１で作っている。

【００８８】この基準クロック発生部２１で作られた基準クロックはデータ入出力インターフェース部３０へ送られ、この基準クロックに従ってＥＣＣエラー訂正された再生情報が後述する情報記録再生部２００から取り出される。更にこの基準クロックに従って暗号化処理が施され、この基準クロックのタイミングで暗号化された情報が外部伝送データ記憶部２５に記憶される。

【００８９】データ伝送インターフェース部８で処理実行されるタイミングはこの基準クロック発生部２１で作られた基準クロックのタイミングとは異なり、外部データ伝送インターフェース部１／２：７／６との間で取り交わされる通信プロトコルのタイミングに沿って処理実行される。またデータ伝送インターフェース部８ではこの通信プロトコルのタイミングに従って外部伝送データ記憶部２５に記憶して有る暗号化情報を取り出し、外部へ転送する。

【００９０】外部伝送データ記憶部２５はバッファとして作用しオーディオデータ等の間欠もキープできる。

【００９１】［３－７］通信用プロトコル変換とタイミング確保

“［２－５］プログラムソフトにおける記録内容と認証相手設定との関係”で記述したように音声情報やビデオ情報を含む混在情報を同時に伝送する場合には、音声情報やビデオ情報が途中で途切れないように一定周期で特定量以上の音声情報やビデオ情報を時分割伝送する必要がある。このようにデータ伝送インターフェース部８でプロトコル変換を行う時にデータ構造の組み替えを行っている。

【００９２】“［２－１］ＤＶＤ-ビデオにおけるフォーマット構造”で説明したようにＤＶＤ-ビデオではＭＰＥＧ２のＰＳ（プログラム　ストリーム）構造に従って情報記録媒体２０１上に情報が記録されている。しかし“［１－４］ネットワークシステムにおける情報伝送の具体例”や“［１－５－１］ＰＣ内の記録装置”に示

したような利用方法の場合には外部データ伝送インターフェース部１／２：７／６との間で送受信する情報のフォーマット構造はＴＳ（トランスポート　ストリーム）が望ましい。ＴＳは１８８バイト固定長の比較的短いパケット単位を使用し、ＰＳとはパケットサイズ、パケット構造が異なる。（藤原洋：最新ＭＰＥＧ教科書（アスキー出版局、１９９４年）Ｐ.２４８）

また外部データ伝送インターフェース部１／２：７／６とデータ伝送インターフェース部８間の通信回線の混雑状況に応じて送受信できる情報の転送レートが大きく影響を受ける。

【００９３】このように外部との送受信情報をリアルタイムで情報記録媒体２０１に記録または情報記録媒体２０１からの再生をおこなう事は難しい。

【００９４】図２のように外部との間で送受信する暗号化情報を外部伝送データ記憶部２５に一時保管し、更に内部に持つ独自のクロックに従って暗号化情報を独立して作成する事により“プロトコル変換時の適応性”“”外部通信回線混雑状況に対する柔軟性”を向上させている。

【００９５】［4］ＡＴＡＰＩ／ＳＣＳＩコマンド

［４－１］記憶装置の標準Ｉ／Ｆ

ＨＤＤ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＭＯ、ＰＤ、ＭＴなどコンピュータシステム内の記録装置に関する標準インターフェースとしてＡＴＡＰＩやＳＣＳＩが存在している。

【００９６】各記憶装置とＰＣのメインＣＰＵ間ではＡＴＡＰＩやＳＣＳＩで決められたコマンドに従って情報の入出力や制御を行っている。

【００９７】ＡＴＡＰＩおよびＳＣＳＩ上で動く認証作業に関する標準コマンドとしては“リポートキーコマンド”と“センドキーコマンド”が存在している。

【００９８】［４－２］コマンド形態

リポートキーコマンド／センドキーコマンドとも共通のコマンド形態として

◎“コマンド文”とその後に続く“データフォーマット”で構成される

◎コマンド文の中には“オペレーションコード”“ＡＧＩＤ（オーセンティケーション　グラント　ＩＤ）”“キーフォーマット”が含まれる（ＡＧＩＤに関する説明は後述する）と言う特徴がある。

【００９９】［４－３］リポートキーコマンド

リポートキーコマンドとは認証相手２～５に情報を送信する時に使うコマンドでオペレーションコードは１６進数で“Ａ４”である。

【０１００】○キーフォーマットが“０００００”で“ＡＧＩＤ”“ストリームＩＤ”“設定エリア情報”を送信し、

○キーフォーマットが“０００００１”で“チャレンジキー”を送信し、

○キーフォーマットが“０００００”で“暗号化キー１”を送信する。

【０１０１】（“［5］暗号鍵”で上記暗号鍵（各種キー）に付いての説明を行う）

［４－４］センドキーコマンド

センドキーコマンドとは認証相手２～５から情報を受信する時に使うコマンドでオペレーションコードは１６進数で“Ａ３”である。

【０１０２】○キーフォーマットが“０００００１”で“チャレンジキー”を送信し、

○キーフォーマットが“００００１１”で“暗号化キー２”を送信する。

【０１０３】（“［5］暗号鍵”で上記暗号鍵（各種キー）に付いての説明を行う）

［5］暗号鍵

［５－１］暗号鍵の種類

図５に示すように一連の認証作業には“ストリームキー”“エリアキー”“チャレンジキー”“暗号化キー１”“暗号化キー２”“バスキー”の６種類の鍵が使われる。

【０１０４】［５－２］バスキー（暗号化して情報を送る際の共通鍵）

“［１－２］複数の外部接続相手との間の情報伝送方法”で説明したように認証相手２～５に対して『暗号化情報の伝送』と『暗号化用の鍵の共有』を行っている。情報記録媒体２０１に記録する情報または情報記録媒体２０１から再生する情報の暗号化／復号化に用いられる暗号鍵を示す。上記暗号化部／復号化部／時変情報発生部２３で用いられる。

【０１０５】暗号化技術は米国の輸出規制の対象になっている。現在ＲＳＡ技術（暗号化方式の一つでアシンメトリックな公開鍵を用いる）では５６ビット程度の暗号強度で有れば輸出可能であるが、それ以上のレングスでは輸出が難しい。また日本を対象とした米国輸出規制ではＤＥＳ（暗号化方式の一つでシンメトリックな共通鍵を用いる）の暗号強度の限界を５６ビットと定めている。同様にＲＣ４やＲＣ２（暗号化方式の一つでシンメトリックな共通鍵を用いる）の暗号強度の限界も５６ビットと定めている。（杉本隆洋：イントラ&インターネットセキュリティ（オーム社１９９６年）Ｐ.１）以上から米国の輸出規制を考慮に入れるとバスキーサイズは５６ビットを標準に考える必要がある。しかし暗号鍵サイズが小さくなると大幅にセキュリティー確保（ハッカーによる暗号鍵の解読防止）が難しくなる。上記の状況を考えバスキーサイズは５６ビットの半分である２８ビット以上が望ましく、セキュリティー確保の観点から最低でも５６ビットの１／４である１４ビット以上は必要である。

【０１０６】［５－３］暗号化キー１／２（バスキーを作るためのキー）

バスキーを作成するために、事前にバスキー作成の元になる鍵情報を相互に交換し合う。認証相手２～５に送信する鍵情報を“暗号化キー１”、認証相手２～５から受信する鍵情報を“暗号化キー２”と呼ぶ。認証相手２～５側と認証機能部９内で同一のルールに従って暗号化キー１と２を合成してバスキーを作成する。

【０１０７】上述した内容と同じ理由で暗号化キー１／２のサイズは２８ビット以上が望ましく、最低でも１４ビット以上は必要である。

【０１０８】［５－４］チャレンジキー（暗号化キー１／２を暗号化するためのキー）

暗号化キー１と２を生のままで送受信すると通信回線から傍受され、暗号化情報を容易に解読されてしまう。それを防止するため暗号化キー１と２自体を暗号化して伝送する。この暗号化キー１／２を暗号化するための暗号鍵をチャレンジキーと呼ぶ。

【０１０９】暗号化キー１／２を送受信する前に、通信回線を使ってチャレンジキーを相互交換する。

【０１１０】［５－５］ストリームキー（チャレンジキーを暗号化するためのキー）

セキュリティー確保のためチャレンジキーを用いても、チャレンジキー自体通信回線を使って伝送されるので、通信回線内の情報をすべて傍受していれば第３者が容易に暗号解読できる。さらにセキュリティー確保を強力にするため“ストリームキー”と“エリアキー”を使っている。

【０１１１】ストリームキーとは情報の種類毎に決められた暗号鍵の事を言う。例えば認証相手Ａ２をＭＰＥＧエンコード／デコードボード、認証相手Ｂ３をオーディオエンコード／デコードボードとするとビデオストリームに対応したＭＰＥＧエンコード／デコードボードのみ共通の暗号鍵を事前に設定しておく。この暗号鍵情報は認証相手Ａ２は知っているが、認証相手Ｂ３は知らない。従ってこの鍵で暗号化した情報を認証相手Ｂ３が傍受しても暗号を解読できない。

【０１１２】ストリームキーは図２の認証情報記憶部２４にあらかじめ記憶されている。このストリームキーは情報内容に応じて対応する個々の認証相手２～５とそれぞれ共有化し、その情報は図６の情報ａ～ｄ対応のストリームキー情報３１～３４としてあらかじめ記録されている。

【０１１３】［５－６］エリアキー（チャレンジキーを暗号化するためのキー）

例えばＭＰＥＧエンコード／デコードボードは情報記録再生装置１に直接接続されるＰＣ（ Personal Computer ）だけでなく、ネットワークを介してつながっている他のＰＣ（クライアント）の中にも装備されている。従ってストリームキーだけでは他のＰＣ内のＭＰＥＧエンコード／デコードボードにより情報を傍受される危険性がある。それを回避するためエリアキーが存在する。

【０１１４】エリアキーとは

○情報記録再生装置１が直接接続されるＰＣシステムの範囲内

○ＴＶやステレオなどのオーディオ・ビデオ機器も含めた個別システム（例えば１本のＩＥＥＥ１３９４で接続されたシステム）の範囲内

○特定のファイーウォール（企業内ＬＡＮの保護システム）内のローカルエリア（例えばファイアウォールで守られた１企業内、１学校内、１役所内、１地域内）の範囲内

○ワールドワイド領域に分類され、それぞれのエリアに応じて特定の共通鍵を持つ。エリアキーは事前に設定され、図６に示すように第１～４エリアキー情報３１～３４位置に記録されている。

【０１１５】エリアキーとストリームキーサイズは暗号化キー１／２のサイズの半分である。エリアキーとストリームキーをＭＳＢ、ＬＳＢとして並べてつなげたコードをチャレンジキーの暗号鍵として利用する。

【０１１６】従ってエリアキーとストリームキーサイズは上述した理由から１４ビット以上が望ましく、最低でも５ビット以上は必要となる。

【０１１７】［６］１個の認証相手との間で行われる認証手順

［６－１］図５についての注釈

“［１－３］複数の外部接続相手との事前の認証作業”に示した事前の認証作業手順について図５を用いて詳細に説明する。

【０１１８】各認証相手２～５との間に行われる認証作業はＡＴＡＰＩもしくはＳＣＳＩ上のコマンドの交換（リポートキーコマンドまたはセンドキーコマンド）により実施される。図５のフローチャートの各ステップの内、リポートキーコマンドによる送信に対応した部分を（ＲＫ）で表示し、センドキーコマンドによる受信に対応した部分を（ＳＫ）で示している。

【０１１９】［６－２］認証相手の設定

情報記録媒体２０１としてＤＶＤ-ビデオを用いた場合を例に取り、認証相手の設定方法について説明する。

【０１２０】情報記録媒体２０１の再生情報から情報の種類を判別するＳ１０１のステップでは“［２－４］ＤＶＤ－ビデオにおける情報内容の識別方法”で説明したように図４のパケット１２内に記録されているストリームＩＤもしくはサブストリームＩＤからパック１０ａ～１０ｄ毎の情報種類を識別する。次に情報種類に応じてＡＧＩＤの割り付けＳ１０２を行う（詳細内容については“［７－２］同時並行認証方法”で説明する）。情報記録再生装置１が接続されているシステム規模に応じて認証処理制御部２２で自動的に伝送対象エリアを設定Ｓ１０４し、それに対応したエリアキー情報３５～３８を認証情報記憶部２４から再生し、そのアドレスを認証処理制御部２２に通知する。更に上記識別した情報種類に

合わせてストリームキーを認証情報記憶部２４から読み取りＳ１０５、そのアドレスを認証処理制御部２２に通知する。

【０１２１】［６－３］認証相手の探索と本人認証
この時点では認証相手Ａ２～認証相手Ｄ５の内、どの相手が該当するか分からない。“［４－３］レポートキーコマンド”で説明したようにレポートキーコマンドを用いて全認証相手２～５に対して同時に“ＡＧＩＤ”“ストリームＩＤ”“設定エリア情報”を送信する。

【０１２２】該当する認証相手Ａ２は“ストリームＩＤ”と“設定エリア情報”から独自に“ストリームキー”と“エリアキー”を割り出し、その２個のキーをつなげて合成キーを作成し、その合成キーを用いて暗号化したチャレンジキーを送信するＳ１０７。

【０１２３】認証機能部９はこのチャレンジキーを受信すれば該当する認証相手Ａ２の候補が存在する事を知る。またこれと平行して認証機能部９内部で独自に“ストリームキー”と“エリアキー”を割り出して合成キーを作成し、この合成キーを用いて暗号化したチャレンジキーの解読（復号化）を行う。正確に解読（復号化）出来れば送信相手が本物の認証相手Ａ２で有ると分かる。

【０１２４】［６－４］チャレンジレスポンス
“［５］暗号鍵”で説明した“暗号化キー１”“暗号化キー２”の送受信には暗号化した情報を送信し、受信側で復号化するステップを踏む。

【０１２５】暗号化技術において双方向本人認証方法として
○ＡからＢへ特定情報を送る
○Ｂはその情報を用いて暗号化した情報をＡにもどす
○Ｂから戻った情報から、Ｂが本人であることをＡが確認する
○ＢからＡへ特定情報を送る
○Ａはその情報を用いて暗号化した情報をＢにもどす
○Ａから戻った情報から、Ａが本人であることをＢが確認すると言う方法が知られており、この方法を“チャレンジレスポンス”と言う。

【０１２６】認証機能部９でもこの“チャレンジレスポンス”を実施している。暗号化部／復号化部／時変情報発生部２３で“暗号化キー１”を作成すると共に、それを認証相手Ａ２から受信したチャレンジキーで暗号化して、認証相手Ａ２に送信するＳ１０８。

【０１２７】次に暗号化部／復号化部／時変情報発生部２３でチャレンジキーを作成し、それを“ストリームキー”と“エリアキー”から作成した合成キーを用いて暗号化して認証相手Ａ２～認証相手Ｄ５に同時に送信するＳ１０９。“ストリームキー”と“エリアキー”を知っている本物の認証相手Ａ２のみがこのチャレンジキーを解読できる。

【０１２８】認証相手Ａ２は独自に“暗号化キー２”を作成し、受信したチャレンジキーを用いてそれを暗号化して返信するＳ１１０。

【０１２９】［６－５］バスキー生成と暗号化情報伝送
この一連のステップにより得られた“暗号化キー１”と“暗号化キー２”から“バスキー”を生成するＳ１１１。この認証作業を完了させるとバスキーで伝送したい情報を暗号化し、“［３－７］通信用プロトコル変換とタイミング確保”で説明したようにトランスポートストリームにプロトコル変換して伝送するＳ１１２。

【０１３０】［７］複数の認証相手と行う同時並行認証方法
［７－１］複数の認証相手との同時処理必要性
情報記録媒体２０１に記録／再生する情報は図３に示すようにパック毎に複数の情報種類が含まれている。また図２に示すように認証相手２～５が複数存在する。従って複数の認証相手２～５と同時に並行して認証作業および情報の伝送を行う必要がある。

【０１３１】［７－２］同時並行認証方法
同時並行認証方法として別々の認証相手２～５と行う各認証ステップ（図５）毎に認証情報記憶部２４に履歴を残す。

【０１３２】認証情報記憶部２４内に記憶した履歴情報内容を図６に示す。認証機能部９では同時に４個の認証相手と認証作業および情報の伝送を行う事ができる。それぞれの認証作業毎にＩＤ番号（ＡＧＩＤ）を割り当てて管理を行う。図６では各ＡＧＩＤ番号４０～４３毎に認証履歴を縦方向（列方向）に記録する。

【０１３３】認証作業とその後に行われる情報の伝送処理が完了すると、対応するＡＧＩＤの列の情報をクリアし、ＡＧＩＤ番号を解放する。

【０１３４】特定のＡＧＩＤ番号の処理が継続中に、新たな認証作業が発生すると認証処理制御部２２は認証情報記憶部２４内の空きＡＧＩＤ番号を探し、そこの列に認証履歴を記憶する。もし空きＡＧＩＤ番号が無い場合には認証不可能の情報をホストＰＣに通知するＳ１０３。このＡＧＩＤ番号の割り付けステップが図５のステップＳ１０２に相当する。

【０１３５】ＡＧＩＤ番号４０～４３毎の認証履歴としては、相手が発行するチャレンジキー情報４５～４８、自分が発行するチャレンジキー情報５１～５４、自分が発行する暗号化キー１情報５５～５８、相手が発行する暗号化キー２情報６０～６３、バスキー情報６５～６８、ＡＧＩＤ送信完了情報７０～７３、チャレンジキー受信完了情報７５～７８、暗号化キー１送信完了情報８０～８３、チャレンジキー送信完了情報８５～８８、暗号化キー２受信完了情報９０～９３からなっている。

【０１３６】［８］認証作業時の具体的信号の流れ
［８－１］認証処理制御部の内部構造
認証処理制御部２２はＣＰＵとそのＣＰＵを制御するプログラムを記憶した半導体メモリ（ＲＡＭ）から構成することが出来る。しかしここではより細かい信号の流れ

や機能を説明するため、認証処理制御部２２を形成する各機能ブロック構成を図７に示し、演算処理部１００、演算実行プログラム解読部１０１、算実行プログラムアドレス指定部１０２、演算実行プログラム記憶部１０３から構成されている。

【０１３７】［８－１－１］演算実行プログラム記憶部１０３の機能

図５のフローチャートを実施するための演算実行プログラムが演算実行プログラム記憶部１０３に記憶されている。

【０１３８】［８－１－２］演算処理部１００の機能

この演算実行プログラムに従って演算処理部１００では

１）データ入出力インターフェース部３０からの再生情報の伝送処理

データ入出力インターフェース部３０への記録情報の伝送処理

２）暗号化部／復号化部／時変情報発生部２３での“暗号化処理”“復号化処理”“各種暗号鍵の作成処理”などの制御

３）暗号化情報の外部伝送データ記憶部２５への記憶処理

外部伝送データ記憶部２５からの暗号化情報の再生処理などを行うと共に

４）認証情報記憶部２４に対する各種暗号鍵の一時保管や各ステップでの認証処理履歴の逐一保存をする事により複数の認証相手２～５との同時並行認証処理を可能にしている。

【０１３９】［８－１－３］演算実行プログラム解読部１０１

演算実行プログラム記憶部１０３に記憶されている演算実行プログラムに対するプログラムコンパイルを演算実行プログラム解読部１０１内で行い、その結果を演算処理部１００に伝送している。また演算実行プログラム解読部１０１では図５のフローチャートに従ったタイミング制御も行っている。

【０１４０】［８－１－４］演算実行プログラムアドレス指定部１０２

複数の認証相手２～５との同時並行認証処理を行う場合、認証相手２～５毎に図５に示した認証ステップが異なる。例えば特定の時刻で見た場合、認証相手Ａ：２に対しては“認証相手Ａ：２に割付けたＡＧＩＤ値の送信処理Ｓ１０６”が完了し、認証相手Ｂ：３ではすでに“こちら側のチャレンジキーで暗号化した“暗号化キー２”の受信Ｓ１１０”まで進み、認証相手Ｃ：４には“認証相手Ｃ：４から暗号化されたチャレンジキーを受信Ｓ１０７”した所と言う場合がある。この直後に行う演算処理部１００の処理は

ａ）始めに認証相手Ｃ：４に対して“認証相手Ｃ：４のチャレンジキーで暗号化した“暗号化キー１”を送信Ｓ１０８”し、

ｂ）次に認証相手Ｂ：３に対して“暗号化キー１”と“暗号化キー２”から“バスキー”を生成Ｓ１１１し、その結果を認証情報記憶部２４に記憶した後でデータ入出力インターフェース部３０から認証相手Ｂ：３に対応したｂパック１０ｂ（図３）内のストリーム情報を読み込み、暗号化部／復号化部／時変情報発生部２３で暗号化させて逐一外部伝送データ記憶部２５に記憶する。

【０１４１】ｃ）“認証相手Ａ：２から暗号化されたチャレンジキーを受信Ｓ１０７”したら上記の（ｂ）の処理を中断して、“認証相手Ａ：２のチャレンジキーで暗号化した“暗号化キー１”を送信Ｓ１０８”する処理を行った後、“認証相手Ａ：２に暗号化されたこちら側のチャレンジキーを送信Ｓ１０９”する処理を行う。その後上記の（ｂ）の処理を継続する。

【０１４２】上記の例から分かるように認証情報記憶部２４に記憶した認証履歴に応じて複数の認証相手２～５に対して個々に図５のフローチャート上の異なるステップ処理を行う必要がある。上記の例を取れば、（ａ）～（ｃ）のステップ毎に演算実行プログラム記憶部１０３上のプログラムが記憶されているアドレスが異なる。（ａ）から（ｂ）、（ｂ）から（ｃ）のステップにすぐに移行できるように演算実行プログラムアドレス指定部１０２によりジャンプするプログラムのアドレス指定を行っている。

【０１４３】［８－２］暗号化部／復号化部／時変情報発生部２３の特徴

［８－２－１］暗号化部／復号化部／時変情報発生部２３の動作上の大きな特徴暗号化部／復号化部／時変情報発生部２３は、図８に示すように、ランダム信号発生器１０４、信号合成器１０５、入出力信号切り替え制御器１０６から構成されている。

【０１４４】暗号化部／復号化部／時変情報発生部２３内で行う“情報の暗号化処理”“暗号化情報の復号化（暗号解読）処理”と“各種暗号鍵の基になる時変情報の発生”処理は、共に機能的に類似した処理を行っている。そのため上記の３つの処理を１組のランダム信号発生器１０４と信号合成器１０５で兼用している所に第１の大きな特徴を持つ。従来上記３つの処理を別々の回路を用いて行っていたのに対し、図８のように兼用化する事により大幅な回路の簡素化とその結果としての低価格化が達成できる。

【０１４５】更にこのランダム信号発生器１０４を単なるシフトレジスタ１０９ａ～ｄ列と見なして信号合成器１０５との組み合わせにより

◎“エリアキー”と“ストリームキー”から“個々の認証相手との合成キー”の作成と

◎“暗号化キー１”と“暗号化キー２”からの“バスキー”の合成を行っている所にも第２の特徴が有る。これにより同様に大幅な回路の簡素化とその結果としての低価格化が達成できる。

【０１４６】［８－２－２］ランダム信号発生器１０４
図８に示すようにシフトレジスタ１０９ａ～ｄと演算器１０８ａ、１０８ｂとセレクタ１０７によりランダム信号発生器１０４が構成されている。

【０１４７】演算器１０８ａ、１０８ｂは排他的論理和回路である加算器から成る。セレクタ１０７により演算器１０８ａの出力信号ｉ３がシフトレジスタ１０９ａの入力ｉ４に接続されている時はランダム信号発生器１０４を形成する。

【０１４８】すなわちシフトレジスタ１０９ａの出力信号はシフトレジスタ１０９ｂの入力に入り、それが続いて信号がシフトレジスタ１０９ｄへ伝わる。シフトレジスタ１０９ｄの出力信号ｉ５は演算器１０８ｂでシフトレジスタ１０９ｃの出力信号と加算され、その加算結果が更に演算器１０８ａでシフトレジスタ１０９ｂの出力信号と加算され、その結果が再びシフトレジスタ１０９ａに入力されて信号が循環する。この循環の結果、シフトレジスタ１０９ｄの出力信号ｉ５はランダム信号に成っている。このランダム信号発生器１０４の組み合わせを最適化すると“M系列のランダム信号発生器”になる。

【０１４９】［８－２－３］信号合成器１０５
一般には信号合成器１０５は暗号化／復号化方式や“バスキー”作成方式に応じて複雑なゲートの組み合わせで構成される。但し、この信号合成器１０５は１個の排他的論理和回路である加算器のみで構成しても暗号化部／復号化部／時変情報発生部２３としての機能は達成できる。

【０１５０】［８－３］認証作業時の具体的信号の流れ
図５に示したフローチャートの各ステップでの具体的信号の流れに付いて以下に説明する。

【０１５１】１）ランダム信号発生器１０４の起動処理
情報記録再生装置１の電源を入れると認証処理制御部２２の制御によりセレクタ１０７にイニシャライズとして“０”の連続が送られる。“０”の連続の伝送がシフトレジスタ１０９内を一巡するとシフトレジスタ１０９ｄの出力ｉ５が再度シフトレジスタ１０９ａの入力ｉ４に戻され、基準クロック発生器２１の発生するクロックに同期して時変情報としてのランダム信号が発生する。

【０１５２】２）ＡＧＩＤの割付け
図３に示した情報記録媒体２０１中に記録されたパック列の中から図４内のパケット１２内のストリームＩＤとサブストリームＩＤを読み取り、必要なＡＧＩＤ数を調べる。認証処理制御部２２では認証情報記憶部２４内の“ＡＧＩＤ送信完了情報７０～７３”を読み取り、空いている（まだ認証処理に使われてない）ＡＧＩＤ番号を探す。各情報種類（ストリーム内容）毎にあいている所にＡＧＩＤを設定する。（以後、例として“ＡＧＩＤ＝０”の列を使って説明を行う。また認証相手として認証相手Ａ：２が該当すると仮定する。）

３）エリアキーとストリームキーの設定
“［５－５］ストリームキー”“［５－６］エリアキー”“［６－２］認証相手の設定”で説明した手順に従ってストリームキーとエリアキーを設定する。ストリームキーは認証情報記憶部２４内の情報ａ～ｄ対応のストリームキー情報３１～３４の中から選択し、エリアキーは認証情報記憶部２４内の第１～４エリアキー情報３５～３８の中から選択する。

【０１５３】（以後、例として情報ｂ対応のストリームキー情報３２と第１エリアキー情報３５を使った場合について説明する）

４）ＡＧＩＤの送信処理
認証処理制御部２２では設定したＡＧＩＤ番号とともに“ストリームＩＤ”と“設定エリア情報”をデータ伝送インターフェース部８に通知する。

【０１５４】通知が完了すると認証処理制御部２２は認証情報記憶部２４内のＡＧＩＤ送信完了情報７０部分に“１”のビット（フラグ）を立てる。

【０１５５】データ伝送インターフェース部８では通知された“ＡＧＩＤ番号”“ストリームＩＤ”“設定エリア情報”をＡＴＡＰＩまたはＳＣＳＩのレポートキーコマンド のフォーマットに合わせてフォーマット変更し、認証相手Ａ：２に送信する。

【０１５６】５）認証相手Ａ：２からの暗号化されたチャレンジキーの受信
ＡＧＩＤを受信すると認証相手Ａ：２はチャレンジキーを発行し、ストリームキーとエリアキーから作った合成キーでそれを暗号化し、ＡＴＡＰＩまたはＳＣＳＩの Send Key Command のフォーマットに合わせて送信する。

【０１５７】データ伝送インターフェース部８では暗号化された認証相手Ａ：２が作成したチャレンジキーをＡＴＡＰＩまたはＳＣＳＩのセンドキーコマンドのフォーマットから抜き出し、外部伝送データ記憶部２５に記憶する。

【０１５８】６）時変情報の一時待避処理
認証相手Ａ：２から受信したチャレンジキー復号化（解読）に先立ち、ランダム信号発生器１０４で発生する情報を認証情報記憶部２４内に一時的に待避させる。すなわち認証処理制御部２２からの指令で入出力信号切り替え制御器１０６はシフトレジスタ１０９ｄ出力ｉ５を直接取り込み、バスライン２４５を経由して認証情報記憶部２４内の“ランダム信号発生器１０４で作られるタイムリーな時変情報３９”（図６）に一時的に保存される。

【０１５９】７）合成キー作成とチャレンジキーの復号化処理
演算実行プログラム記憶部１０３内のプログラムに従い、演算処理部１００では認証情報記憶部２４内の情報ｂ対応のストリームキー情報３２をバスライン２６を経由して暗号化／復号化／時変情報発生部２３へ伝送す

る。暗号化／復号化／時変情報発生部２３内では入出力信号切り替え制御器１０６がセレクタ１０７を制御して情報ｂ対応のストリームキー情報３２をそのままシフトレジスタ１０９ａへ送る。その直後にそれに続いて認証情報記憶部２４内の第１エリアキー情報３５をシフトレジスタ１０９ａへ送る。この時も前述した方法と同様な方法でシフトレジスタ１０９ａへ送る。

【０１６０】第１エリアキー情報３５をシフトレジスタ１０９ａへ伝送完了時点で、情報ｂ対応のストリームキー情報３２の最初のビットがシフトレジスタ１０９ｄの最上位ビット位置に来ており、このシフトレジスタ１０９ａ～ｄ内の情報が合成キーになる。

【０１６１】引き続き認証処理制御部２２の制御により外部伝送データ記憶部２５に記憶されている“暗号化されたチャレンジキー”が信号合成器１０５の入力信号ｉ２として入力されるように入出力信号切り替え制御器１０６が働く。その結果、信号合成器１０５の出力信号ｉ６に復号化（解読）されたチャレンジキーが現れる。その後、復号化（解読）されたチャレンジキー情報はシフトレジスタ１１０ａ～ｄ、入出力信号切り替え制御器１０６、バスライン２５４を経由して認証情報記憶部２４内の“相手が発行するチャレンジキー情報４５”のアドレスに記憶される。

【０１６２】上記の説明では第１エリアキー情報３５のシフトレジスタ１０９ａへの伝送完了直後に暗号化されたチャレンジキーの復号化（解読）が開始されているが、それに限らずシフトレジスタ１０９ａへの伝送完了後、特定のクロックを経た後で復号化を開始するように設定する事も可能である。

【０１６３】このように復号化後のチャレンジキーの認証情報記憶部２４内への記憶が完了すると、チャレンジキー受信完了情報７５のビット（フラグ）を“１”にする。

【０１６４】８）時変情報発生の再開処理

ＡＧＩＤ番号の暗号化処理が完了すると暗号化部／復号化部／時変情報発生部２３は時変情報発生の再開を行う。すなわち認証情報記憶部２４内に一時的に保管されたランダム信号発生器で作られるタイムリーな時変情報３９（図６）は認証処理制御部２２の制御に応じてバスライン２６、入出力信号切り替え制御器１０６、セレクタ１０７を経てシフトレジスタ１０９ａへ入力される（ｉ４）。入力が完了するとセレクタ１０７が閉じて演算器１０８ａの出力信号ｉ３をシフトレジスタ１０９の入力信号ｉ４へ戻し、再び時変情報であるランダム信号を継続して発生させる。

【０１６５】９）暗号化キー１の作成

通常はランダム信号発生器１０４で常に時変情報を発生しているので、特定のタイミングでその時変情報を取り出す事により各種の暗号化鍵を作成できる。

【０１６６】演算実行プログラム記憶部１０３内のプログラムに従い、演算処理部１００の指令に応じてランダム信号発生器１０４の出力信号ｉ５が“暗号化キー１”として入出力信号切り替え制御器１０６に入力され、バスライン２６を経由して認証情報記憶部２４内の“自分が発行する暗号化キー１情報５５”（図６）に記憶される。暗号化キー１の記憶が完了すると“６）時変情報の一時待避処理”が行われる。

【０１６７】１０）暗号化キー１の暗号化方法

認証処理制御部２２の制御に従い、認証情報記憶部２４内の“相手が発行するチャレンジキー情報４５”のアドレスからチャレンジキーをバスライン２６、入出力信号切り替え制御器１０６、セレクタ１０７を経由してシフトレジスタ１０９ａの入力部ｉ４に入力される。入力が完了するとその信号が信号合成器１０５の入力部ｉ５に入力される。

【０１６８】その後、セレクタ１０７を閉じて特定クロック分だけランダム信号発生器１０４内を循環させた後、認証情報記憶部２４内の“自分が発行する暗号化キー１情報５５”のアドレスからバスライン２６、入出力信号切り替え制御器１０６を経由してもう一方の信号合成器１０５の入力部ｉ２に入力させる。信号合成器１０５の出力信号ｉ６が暗号化された暗号化キー１となり、入出力信号切り替え制御器１０６バスライン２６を経て外部伝送データ記憶部２５に記憶される。

【０１６９】暗号化された暗号化キー１の作成が完了すると認証情報記憶部２４内の“暗号化キー１送信完了情報８０”のアドレスのビット（フラグ）を“１”にした後、“８）時変情報発生の再開処理”に戻る。

【０１７０】１１）暗号化キー１の送信処理

データ伝送インターフェース部８では外部伝送データ記憶部２５から暗号化された暗号化キー１を読み取り、ＡＴＡＰＩまたはＳＣＳＩのレポートキーコマンドのフォーマットに合わせてフォーマット変更し、認証相手Ａ：２に送信する。

【０１７１】１２）チャレンジキーの送信処理

“９）暗号化キー１の作成”と同じ方法でチャレンジキーを作成し、“自分が発行するチャレンジキー情報５０”のアドレスに保存する。次に“７）合成キー作成とチャレンジキーの復号化処理”と同じ方法で合成キーをシフトレジスタ１０９ａ～ｄにロードすると共に、チャレンジキーの暗号化を行う。

【０１７２】なお、同一の暗号鍵をシフトレジスタ１０９ａ～ｄにロードした場合、信号合成器１０５の入力ｉ２に元の信号を入力すると出力信号ｉ６として暗号化されると共に、信号合成器１０５の入力ｉ２に暗号化された信号を入力すると出力信号ｉ６として復号化（解読された）信号が得られる。暗号鍵信号として“０”にしろ“１”にしろ同じ信号を２回加算すると結果は元の信号に戻るため。

【０１７３】その後、暗号化されたチャレンジキーを外

部伝送データ記憶部２５に記憶し、“チャレンジキー送信完了情報８５”のアドレスのビット（フラグ）を“１”にする。また“８）時変情報発生の再開処理”に戻る。

【０１７４】更に“１１）暗号化キー１の送信処理”と同様にレポートキーコマンドで認証相手Ａ：２に送信する。

【０１７５】１３）バスキーの生成処理

“５）認証相手Ａ：２からの暗号化されたチャレンジキーの受信”と同様に暗号化した“暗号化キー２”を受信すると、“６）時変情報の一時待避処理”を行い、“１０）暗号化キー１の暗号化方法”と同じ方法で“自分が発行するチャレンジキー情報５０”を用いて“暗号化キー２”の復号化（解読）を行い、“相手が発行する暗号化キー２情報６０”アドレスに復号化後の暗号化キー２情報を記憶すると共に“暗号化キー２受信完了情報９０”のアドレスのビット（フラグ）を“１”にする。

【０１７６】次に認証情報記憶部２４から“自分が発行する暗号化キー１情報”をバスライン２６、入出力信号切り替え制御器１０６、セレクタ１０７を経由してシフトレジスタ１０９ａ～ｄの入力部ｉ４へ入力させる。ここでシフトレジスタ１０９ａ～ｄは“自分が発行する暗号化キー１情報”の一時保存場所として使用している。

【０１７７】“自分が発行する暗号化キー１情報”がシフトレジスタ１０９ｄまで埋まると“相手が発行する暗号化キー２情報”をバスライン２６、入出力信号切り替え制御器１０６経由で信号合成器１０５の入力部ｉ２に入力し、信号合成器１０５で暗号化キー１と暗号化キー２の合成を行う。信号合成器１０５出力信号ｉ６がバスキーとなり、認証情報記憶部２４内の“バスキー情報６５”のアドレスに記憶される。

【０１７８】１４）再生情報の暗号化処理

情報記録媒体２０１から再生した情報を暗号化して送信する場合、認証処理制御部２２の制御に従い、次に認証情報記憶部２４から“バスキー情報６５”をバスライン２６、入出力信号切り替え制御器１０６、セレクタ１０７を経由してシフトレジスタ１０９の入力部ｉ４へ入力させる。バスキーの転送が完了するとセレクタ１０７が閉じ、バスキーを出発点として信号がランダム信号発生器１０４内で循環する。再生信号の暗号化が続く限りこの循環は継続される。

【０１７９】情報記録媒体２０１から再生した情報はデータ入出力インターフェース部３０からバスライン２６、入出力信号切り替え器１０６を経て信号合成器１０５の入力部ｉ２に入力され、信号合成器１０５出力である暗号化された情報はｉ６からシフトレジスタ１１０ａ～ｄ、入出力信号切り替え器１０６、バスライン２６を経て外部伝送データ記憶部２５へ記憶される。

【０１８０】１５）複数認証相手との並行処理、割り込み処理

以上１個の認証相手Ａ：２との間の認証手続きについて説明した。上述の説明から明らかなように、各ステップ毎に認証履歴を認証情報記憶部２５に記憶して有るので途中で認証手続きを中断し、他の認証相手Ｂ：３との認証手続きを行うことが出来る。

【０１８１】［９］ネットワークを用いた認証処理方法

［９－１］ＴＣＰ／ＩＰを用いた場合のネットワーク上認証処理

ネットワークシステム上での認証方法については“［１－４］ネットワークシステムにおける情報伝送の具体例”で説明した。ここでは図５に示した認証手順フローチャートの各ステップとネットワーク上の通信内容との対応を通信プロトコルとしてＴＣＰ／ＩＰを例にとって説明する。

【０１８２】“［８］認証作業時の具体的信号の流れ”では情報記録媒体２０１の再生情報から認証処理が開始されるが、ネットワーク上の認証処理では“［１－４］ネットワークシステムにおける情報伝送の具体例”で説明したようにネットワークサーバから情報の配送・収集先のクライアント（のＩＰアドレスや電話番号）と配送・収集する情報内容を通知されて初めて認証処理を開始する。

【０１８３】［９－２］サーバから特定のクライアントを指定された場合

この場合にはクライアントから特定のＩＰアドレスや接続先の電話番号を指定されるので認証相手Ａ：２は事前に固定される。従って図５の“認証相手に割付けたＡＧＩＤの値・エリア情報・ストリームＩＤ情報の送信Ｓ１０６”は事前に固定された相手に対して行われる。この場合にはそれ以降の各ステップは情報伝送時の漏洩防止・セキュリティー確保のための暗号キーの共有化処理となる。具体的な処理内容は“［８－３］認証作業時の具体的信号の流れ”と同じになる。

【０１８４】ネットワークを用いて相手のクライアントに情報を送信するまたはクライアントから情報を受信する場合、経路途中のゲートウェイ（ルーター）で伝送する情報を容易にコピーできる。従って漏洩防止・セキュリティー確保のため共有化した暗号キーを用いて暗号化した情報を伝送する事が非常に重要となる。

【０１８５】［９－３］サーバから同時に複数のクライアントを指定された場合

電子メールを使って複数のクライアントに多量の情報を送付するような場合、サーバから同時に複数のクライアントを指定される事が有る。伝送する情報が機密性の高い場合には個々のクライアントをそれぞれ別々の認証相手Ａ：２～Ｄ：５と考え、個々に通信して認証作業を行う。それ以外は“［９－１－１］サーバから特定のクライアントを指定された場合”と同じ処理になる。［９－４］サーバからクライアント範囲のみを指定された場合ＴＣＰ／ＩＰプロトコルの場合、サーバは自分が通信を

行うクライアントのＩＰアドレスとクライアントマシン名の一覧表を“ｈｏｓｔｓ”と言う名のファイルに保存している。またサーバが管理するネットワークドメインを持ち、そのドメインに含まれるクライアントマシンをＩＰアドレス等で管理している。サーバから情報記録再生装置に対して情報伝送相手のクライアントを指定する代わりに情報を送信するあるいは情報を受信するクライアントの範囲を指定して、その中から該当クライアントを探し、情報を送受信するように要求される場合が有る。この時サーバから情報記録再生装置に対して示されるクライアントの範囲として“ｈｏｓｔｓ”そのものを渡したり、特定のドメインに含まれるクライアントマシンのＩＰアドレスリストを渡す。

【０１８６】図５“認証相手が属するエリアに応じた該当エリアキーの設定Ｓ１０４”はサーバから通知されたネットワークドメインの認識と、ネットワークドメイン毎に事前に設定して有る暗号鍵であるエリアキーの抽出に対応する。ネットワークドメインに対する対応するエリアキーの情報は図２の認証情報記憶部２４に事前に記憶して有る。

【０１８７】認証機能部９では通信機能を有するデータ伝送インターフェース部８を制御してＩＰアドレスリストに含まれる全クライアントに対して同時に図５の“認証相手に割付けたＡＧＩＤの値・エリア情報・ストリームＩＤ情報の送信Ｓ１０６”を送信する。送信する情報によってはクライアントに対してストリームＩＤ情報の代わりに別のフォーマットに基付いたこれから伝送しようとしている情報内容に関する情報を伝送する場合もある。このステップを実施するとネットワーク内の情報配送を受けたいクライアント、もしくは情報送信する必要の有るクライアントから“自己申請”の形で回答が来る。すなわち該当クライアントである“認証相手から暗号化されたチャレンジキーを受信するＳ１０７”の形で回答が来る。ＴＣＰ／ＩＰプロトコルでは必ず通信パケット内に送信側のＩＰアドレスが含まれるので、認証処理制御部２２はその受信した通信パケットから認証相手Ａ：２のＩＰアドレスを取り出して、図２の認証情報記憶部２４に保存する。以後保存したＩＰアドレスを用いて認証相手Ａ：２との認証作業を行う。つまり“認証相手のチャレンジキーで暗号化した“暗号化キー１”を送信Ｓ１０８”以降の全ステップは上記に抽出したＩＰアドレスを持ったクライアントに対してのみ通信を行う。

【０１８８】“認証相手に割付けたＡＧＩＤの値・エリア情報・ストリームＩＤ情報の送信Ｓ１０６”に対して複数のクライアントが該当し、複数のクライアントから回答が来た場合には、ここのクライアントをそれぞれ異なる認証相手Ｂ：３、認証相手Ｃ：４、認証相手Ｄ：５と分けて個々に認証作業を行う。

【０１８９】ネットワーク経路途中での情報の不正コピー、情報漏洩を防止し、セキュリティーを確保するために個々のクライアント毎に異なる認証相手と見なして別々に認証作業を行う事が望ましい。

【０１９０】図５“認証相手のチャレンジキーで暗号化した“暗号化キー１”を送信Ｓ１０８”以降の認証処理の具体的内容は“［８－３］認証作業時の具体的信号の流れ”と基本的に同じ処理となる。

【０１９１】図９を用いて情報記録再生装置１内の情報記録再生部（物理系ブロック）２００の内部構造を説明する。

【０１９２】［１０］情報記録再生部２００の機能説明
［１０－１］情報記録再生部２００の基本機能
情報記録再生部２００では
◎情報記録媒体２０１上の所定位置に集光スポットを用いて新規情報の記録あるいは書き換え（情報の消去も含む）を行う。

【０１９３】◎情報記録媒体２０１上の所定位置から集光スポットを用いてすでに記録されている情報の再生を行う。

【０１９４】の処理を行う。

【０１９５】［１０－２］情報記録再生部２００の基本機能達成手段
上記の基本機能を達成する手段として情報記録再生部２００では
◎情報記録媒体２０１上のトラック（図示して無い）に沿って集光スポットをトレース（追従）させる。

【０１９６】◎情報記録媒体２０１に照射する集光スポットの光量を変化させて情報の記録／再生／消去の切り替えを行う。

【０１９７】◎外部から与えられる記録信号ｄを高密度かつ低エラー率で記録するために最適な信号に変換する。

【０１９８】を行っている。

【０１９９】［１１］機構部分の構造と検出部分の動作
［１１－１］光学ヘッド２０２基本構造と信号検出回路
［１１－１－１］光学ヘッド２０２による信号検出
光学ヘッド２０２は基本的には図示して無いが光源である半導体レーザ素子と光検出器と対物レンズから構成されている。

【０２００】半導体レーザ素子から発光されたレーザ光は対物レンズにより情報記録媒体（光ディスク）２０１上に集光される。情報記録媒体（光ディスク）２０１の光反射膜もしくは光反射性記録膜で反射されたレーザ光は光検出器により光電変換される。

【０２０１】光検出器で得られた検出電流はアンプ２１３により電流ー電圧変換されて検出信号となる。この検出信号はフォーカス・トラックエラー検出回路２１７あるいは２値化回路２１２で処理される。一般的には光検出器は複数の光検出領域に分割され、各光検出領域に照射される光量変化を個々に検出している。この個々の検出信号に対してフォーカス・トラックエラー検出回路２

１７で和・差の演算を行いフォーカスずれとトラックずれの検出を行う。情報記録媒体（光ディスク）２０１の光反射膜もしくは光反射性記録膜からの反射光量変化を検出して情報記録媒体２０１上の信号を再生する。

【０２０２】［１１－１－２］フォーカスずれ検出方法
フォーカスずれ量を光学的に検出する方法として

○非点収差法：情報記録媒体（光ディスク）２０１の光反射膜もしくは光反射性記録膜で反射されたレーザ光の検出光路に図示して無いが非点収差を発生させる光学素子を配置し、光検出器上に照射されるレーザ光の形状変化を検出する方法。光検出領域は対角線状に４分割されている。各検出領域から得られる検出信号に対し、フォーカス・トラックエラー検出回路２１７内で対角和間の差を取ってフォーカスエラー検出信号を得る。　あるいは

○ナイフエッジ法：情報記録媒体２０１で反射されたレーザ光に対して非対称に一部を遮光するナイフエッジを配置する方法。光検出領域は２分割され、各検出領域から得られる検出信号間の差を取ってフォーカスエラー検出信号を得る。のどちらかを使う場合が多い。

【０２０３】［１１－１－３］トラックずれ検出方法
情報記録媒体（光ディスク）２０１はスパイラル状または同心円状のトラックを有し、トラック上に情報が記録される。このトラックに沿って集光スポットをトレースさせて情報の再生もしくは記録／消去を行う。安定して集光スポットをトラックに沿ってトレースさせるため、トラックと集光スポットの相対的位置ずれを光学的に検出する必要がある。トラックずれ検出方法としては一般に

○ＤＰＤ(Differential Phase Detection)法：情報記録媒体（光ディスク）２０１の光反射膜もしくは光反射性記録膜で反射されたレーザ光の光検出器上での強度分布変化を検出する。光検出領域は対角線状に４分割されている。各検出領域から得られる検出信号に対し、フォーカス・トラックエラー検出回路２１７内で対角和間の差を取ってトラックエラー検出信号を得る。　あるいは

○プッシュープル法：情報記録媒体２０１で反射されたレーザ光の光検出器上での強度分布変化を検出する。光検出領域は２分割され、各検出領域から得られる検出信号間の差を取ってトラックエラー検出信号を得る。

【０２０４】○ツインースポット法：半導体レーザ素子と情報記録媒体２０１間の送光系に回折素子などを配置して光を複数に波面分割し、情報記録媒体２０１上に照射する±１次回折光の反射光量変化を検出する。再生信号検出用の光検出領域とは別に＋１次回折光の反射光量と－１次回折光の反射光量を個々に検出する光検出領域を配置し、それぞれの検出信号の差を取ってトラックエラー検出信号を得る。などが有る。

【０２０５】［１１－１－４］対物レンズアクチュエータ構造
半導体レーザ素子から発光されたレーザ光を情報記録媒体２０１上に集光させる対物レンズ（図示されて無い）は対物レンズアクチュエータ駆動回路２１８の出力電流に応じて２軸方向に移動可能な構造になっている。この対物レンズの移動方向は

・フォーカスずれ補正用に情報記録媒体２０１に対する垂直方向に移動し、

・トラックずれ補正用に情報記録媒体２０１の半径方向に移動する。

【０２０６】図示して無いが対物レンズの移動機構を対物レンズアクチュエータと呼ぶ。対物レンズアクチュエータ構造としては

○軸摺動方式：中心軸（シャフト）に沿って対物レンズと一体のブレードが移動する方式で、ブレードが中心軸に沿った方向に移動してフォーカスずれ補正を行い、中心軸を基準としたブレードの回転運動によりトラックずれ補正を行う方法あるいは

○４本ワイアー方式：対物レンズ一体のブレードが固定系に対し４本のワイヤで連結されており、ワイアーの弾性変形を利用してブレードを２軸方向に移動させる方法が多く使われている。いずれの方式も永久磁石とコイルを持ち、ブレードに連結したコイルに電流を流す事によりブレードを移動させる構造になっている。

【０２０７】［１１－２］情報記録媒体２０１の回転制御系
スピンドルモータ２０４の駆動力によって回転する回転テーブル２２１上に情報記録媒体（光ディスク）２０１を装着する。

【０２０８】情報記録媒体２０１の回転数は情報記録媒体２０１から得られる再生信号によって検出する。すなわちアンプ２１３出力の検出信号（アナログ信号）は２値化回路２１２でデジタル信号に変換され、この信号からＰＬＬ回路２１１により一定周期信号（基準クロック信号）を発生させる。情報記録媒体回転速度検出回路２１４ではこの信号を用いて情報記録媒体２０１の回転数を検出し、その値を出力する。

【０２０９】情報記録媒体２０１上で再生あるいは記録／消去する半径位置に対応した情報記録媒体回転数の対応テーブルは半導体メモリ２１９にあらかじめ記録して有る。再生位置もしくは記録／消去位置が決まると、制御部２２０は半導体メモリ２１９情報を参照して情報記録媒体２０１の目標回転数を設定し、その値をスピンドルモータ駆動回路２１５に通知する。

【０２１０】スピンドルモータ駆動回路２１５では、この目標回転数と情報記録媒体回転速度検出回路２１４の出力信号（現状での回転数）との差を求め、その結果に応じた駆動電流をスピンドルモータ２０４に与えてスピンドルモータ２０４の回転数が一定になるように制御する。情報記録媒体回転速度検出回路２１４の出力信号は

情報記録媒体２０１の回転数に対応した周波数を有するパルス信号で、スピンドルモータ駆動回路２１５ではこの信号の周波数とパルス位相の両方に対して制御する。

【０２１１】［１１－３］光学ヘッド移動機構

情報記録媒体２０１の半径方向に光学ヘッド２０２を移動させるため光学ヘッド移動機構（送りモータ）２０３を持っている。

【０２１２】光学ヘッド２０２を移動させるガイド機構として棒状のガイドシャフトを利用する場合が多く、このガイドシャフトと光学ヘッド２０２の一部に取り付けられたブッシュ間の摩擦を利用して光学ヘッド２０２が移動する。それ以外に回転運動を使用して摩擦力を軽減させたベアリングを用いる方法も有る。

【０２１３】光学ヘッド２０２を移動させる駆動力伝達方法は図示して無いが固定系にピニオン（回転ギヤ）の付いた回転モータを配置し、ピニオンとかみ合う直線状のギヤであるラックを光学ヘッド２０２の側面に配置して回転モータの回転運動を光学ヘッド２０２の直線運動に変換している。それ以外の駆動力伝達方法としては固定系に永久磁石を配置し、光学ヘッド２０２に配置したコイルに電流を流して直線的方向に移動させるリニアモータ方式を使う場合もある。

【０２１４】回転モータ、リニアモータいずれの方式でも基本的には送りモータに電流を流して光学ヘッド２０２移動用の駆動力を発生させている。この駆動用電流は送りモータ駆動回路２１６から供給される。

【０２１５】［１２］各制御回路の機能

［１２－１］集光スポットトレース制御

フォーカスずれ補正あるいはトラックずれ補正を行うため、フォーカス・トラックエラー検出回路２１７の出力信号（検出信号）に応じて光学ヘッド２０２内の対物レンズアクチュエータ（図示して無い）に駆動電流を供給する回路が対物レンズアクチュエータ駆動回路２１８である。高い周波数領域まで対物レンズ移動を高速応答させるため、対物レンズアクチュエータの周波数特性に合わせた特性改善用の位相補償回路を内部に有している。

【０２１６】対物レンズアクチュエータ駆動回路２１８では制御部２２０の命令に応じて

◎フォーカス／トラックずれ補正動作（フォーカス／トラックループ）のＯＮ／ＯＦＦ処理

◎情報記録媒体２０１の垂直方向（フォーカス方向）へ対物レンズを低速で移動させる処理（フォーカス／トラックループＯＦＦ時に実行）

◎キックパルスを用いて情報記録媒体２０１の半径方向（トラックを横切る方向）にわずかに動かして、集光スポットを隣のトラックへ移動させる処理を行う。

【０２１７】［１２－２］レーザ光量制御

［１２－２－１］再生と記録／消去の切り替え処理

再生と記録／消去の切り替えは情報記録媒体２０１上に照射する集光スポットの光量を変化させて行う。

【０２１８】相変化方式を用いた情報記録媒体に対しては一般的に

［記録時の光量］＞［消去時の光量］＞［再生時の光量］

の関係が成り立ち、光磁気方式を用いた情報記録媒体に対しては一般的に

［記録時の光量］　［消去時の光量］＞［再生時の光量］

の関係が有る。光磁気方式の場合には記録／消去時には情報記録媒体２０１に加える外部磁場（図示して無い）の極性を変えて記録と消去の処理を制御している。

【０２１９】情報再生時には情報記録媒体２０１上には一定の光量を連続的に照射している。

【０２２０】新たな情報を記録する場合には、この再生時の光量の上にパルス状の断続的光量を上乗せする。半導体レーザ素子が大きな光量でパルス発光した時に情報記録媒体２０１の光反射性記録膜が局所的に光学的変化もしくは形状変化を起こし、記録マークが形成される。すでに記録されている領域の上に重ね書きする場合も同様に半導体レーザ素子をパルス発光させる。

【０２２１】すでに記録されている情報を消去する場合には、再生時よりも大きな一定光量を連続照射する。連続的に情報を消去する場合にはセクター単位など特定周期毎に照射光量を再生時に戻し、消去処理と平行して間欠的に情報再生を行う。間欠的に消去するトラックのトラック番号やアドレスを再生し、消去トラックの誤りが無い事を確認しながら消去処理を行っている。

【０２２２】［１２－２－２］レーザ発光制御

図示して無いが光学ヘッド２０２内には半導体レーザ素子の発光量を検出するための光検出器を内蔵している。半導体レーザ駆動回路２０５ではその光検出器出力（半導体レーザ素子発光量の検出信号）と記録／再生／消去制御波形発生回路２０６から与えられる発光基準信号との差を取り、その結果に基付き半導体レーザへの駆動電流をフィードバックしている。

【０２２３】［１３］機構部分の制御系に関する諸動作

［１３－１］起動制御

情報記録媒体（光ディスク）２０１を回転テーブル２２１上に装着し、起動制御を開始すると、以下の手順に従って処理が行われる。

【０２２４】１）制御部２２０からスピンドルモータ駆動回路２１５に目標回転数が伝えられ、スピンドルモータ駆動回路２１５からスピンドルモータ２０４に駆動電流が供給されてスピンドルモータ２０４の回転が開始する。

【０２２５】２）同時に制御部２２０から送りモータ駆動回路２１６に対してコマンド（実行命令）が出され、送りモータ駆動回路２１６から光学ヘッド駆動機構（送りモータ）２０３に駆動電流が供給されて光学ヘッド２０２が情報記録媒体２０１の最内周位置に移動する。情

報記録媒体２０１の情報が記録されている領域を越えてさらに内周部に光学ヘッド２０２が来ている事を確認する。

【０２２６】３）スピンドルモータ２０４が目標回転数に到達すると、そのステータス（状況報告）が制御部２２０に出される。

【０２２７】４）制御部２２０から記録／再生／消去制御波形発生回路２０６に送られた再生光量信号に合わせて半導体レーザ駆動回路２０５から光学ヘッド２０２内の半導体レーザ素子に電流が供給されてレーザ発光を開始する。

【０２２８】＊情報記録媒体（光ディスク）２０１の種類によって再生時の最適照射光量が異なる。起動時にはそのうちの最も照射光量の低い値に設定する。

【０２２９】５）制御部２２０からのコマンドに従って光学ヘッド２０２内の対物レンズ（図示して無い）を情報記録媒体２０１から最も遠ざけた位置にずらし、ゆっくりと対物レンズを情報記録媒体２０１に近付けるよう対物レンズアクチュエータ駆動回路２１８が制御する。

【０２３０】６）同時にフォーカス・トラックエラー検出回路２１７でフォーカスずれ量をモニターし、焦点が合った位置近傍に対物レンズが来た時ステータスを出して制御部２２０に通知する。

【０２３１】７）制御部２２０ではその通知をもらうと、対物レンズアクチュエータ駆動回路２１８に対してフォーカスループをオンにするようコマンドを出す。

【０２３２】８）制御部２２０はフォーカスループをオンにしたまま送りモータ駆動回路２１６にコマンドを出して光学ヘッド２０２をゆっくり情報記録媒体２０１の外周部方向へ移動させる。

【０２３３】９）同時に光学ヘッド２０２からの再生信号をモニターし、光学ヘッド２０２が情報記録媒体２０１上の記録領域に到達したら光学ヘッド２０２の移動を止め、対物レンズアクチュエータ駆動回路２１８に対してトラックループをＯＮさせるコマンドを出す。

【０２３４】１０）情報記録媒体（光ディスク）２０１の内周部に記録されている“再生時の最適光量”と“記録／消去時の最適光量”を再生し、その情報が制御部２２０を経由して半導体メモリ２１９に記録される。

【０２３５】１１）さらに制御部２２０ではその“再生時の最適光量”に合わせた信号を記録／再生／消去制御波形発生回路２０６に送り、再生時の半導体レーザ素子の発光量を再設定する。

【０２３６】１２）情報記録媒体２０１に記録されている“記録／消去時の最適光量”に合わせて記録／消去時の半導体レーザ素子の発光量が設定される。

【０２３７】［１３－２］アクセス制御

［１３－２－１］情報記録媒体２０１上のアクセス先情報の再生

情報記録媒体２０１上のどの場所にどのような内容の情報が記録されているかに付いての情報は情報記録媒体２０１の種類により異なり、一般的には情報記録媒体２０１内の

◎ディレクトリ管理領域：情報記録媒体２０１の内周領域もしくは外周領域にまとまって記録して有る

　かまたは

◎ナビゲーションパック：ＭＰＥＧ２のＰＳ（プログラム　ストリーム）のデータ構造に準拠したＶＯＢＳ（ビデオ　オブジェクト　セット）の中に含まれ、次の映像がどこに記録して有るかの情報が記録されているなどに記録して有る。

【０２３８】特定の情報を再生あるいは記録／消去したい場合には、まず上記の領域内の情報を再生し、そこで得られた情報からアクセス先を決定する。

【０２３９】［１３－２－２］粗アクセス制御

制御部２２０ではアクセス先の半径位置を計算で求め、現状の光学ヘッド２０２位置との間の距離を割り出す。

【０２４０】光学ヘッド２０２移動距離に対して最も短時間で到達出来る速度曲線情報が事前に半導体メモリ２１９内に記録されている。制御部２２０はその情報を読み取り、その速度曲線に従って以下の方法で光学ヘッド２０２の移動制御を行う。

【０２４１】制御部２２０から対物レンズアクチュエータ駆動回路２１８に対してコマンドを出してトラックループをＯＦＦした後、送りモータ駆動回路２１６を制御して光学ヘッド２０２の移動を開始させる。

【０２４２】集光スポットが情報記録媒体２０１上のトラックを横切ると、フォーカス・トラックエラー検出回路２１７内でトラックエラー検出信号が発生する。このトラックエラー検出信号を用いて情報記録媒体２０１に対する集光スポットの相対速度が検出できる。

【０２４３】送りモータ駆動回路２１６では、このフォーカス・トラックエラー検出回路２１７から得られる集光スポットの相対速度と制御部２２０から逐一送られる目標速度情報との差を演算し、その結果を光学ヘッド駆動機構（送りモータ）２０３への駆動電流にフィードバックかけながら光学ヘッド２０２を移動させる。

【０２４４】“［１１－３］光学ヘッド移動機構”に記述したようにガイドシャフトとブッシュあるいはベアリング間には常に摩擦力が働いている。光学ヘッド２０２が高速に移動している時は動摩擦が働くが、移動開始時と停止直前には光学ヘッド２０２の移動速度が遅いため静止摩擦が働く。この時には相対的摩擦力が増加しているので（特に停止直前には）制御部２２０からのコマンドに応じて光学ヘッド駆動機構（送りモータ）２０３に供給する電流の増幅率（ゲイン）を増加させる。

【０２４５】［１３－２－３］密アクセス制御

光学ヘッド２０２が目標位置に到達すると制御部２２０から対物レンズアクチュエータ駆動回路２１８にコマンドを出してトラックループをＯＮさせる。

【０２４６】集光スポットは情報記憶媒体２０１上のトラックに沿ってトレースしながらその部分のアドレスもしくはトラック番号を再生する。

【０２４７】そこでのアドレスもしくはトラック番号から現在の集光スポット位置を割り出し、到達目標位置からの誤差トラック数を制御部２２０内で計算し、集光スポットの移動に必要なトラック数を対物レンズアクチュエータ駆動回路２１８に通知する。

【０２４８】対物レンズアクチュエータ駆動回路２１８内で１組キックパルスを発生させると対物レンズは情報記憶媒体２０１の半径方向にわずかに動いて、集光スポットが隣のトラックへ移動する。

【０２４９】対物レンズアクチュエータ駆動回路２１８内では一時的にトラックループをＯＦＦさせ、制御部２２０からの情報に合わせた回数のキックパルスを発生させた後、再びトラックループをＯＮさせる。

【０２５０】密アクセス終了後、制御部２２０は集光スポットがトレースしている位置の情報（アドレスもしくはトラック番号）を再生し、目標トラックにアクセスしている事を確認する。

【０２５１】［１３－３］連続記録／再生／消去制御

図９に示すようにフォーカス・トラックエラー検出回路２１７から出力されるトラックエラー検出信号は送りモータ駆動回路２１６に入力されている。上述した“起動制御時”と“アクセス制御時”には送りモータ駆動回路２１６内ではトラックエラー検出信号を使用しないように制御部２２０により制御されている。

【０２５２】アクセスにより集光スポットが目標トラックに到達した事を確認した後、制御部２２０からのコマンドによりモータ駆動回路２１６を経由してトラックエラー検出信号の一部が光学ヘッド駆動機構（送りモータ）２０３への駆動電流として供給される。連続に再生もしくは記録／消去処理を行っている期間中、この制御は継続される。

【０２５３】情報記憶媒体２０１の中心位置は回転テーブル２２１の中心位置とわずかにずれた偏心を持って装着されている。トラックエラー検出信号の一部を駆動電流として供給すると、偏心に合わせて光学ヘッド２０２全体が微動する。

【０２５４】また長時間連続して再生もしくは記録／消去処理を行うと、集光スポット位置が徐々に外周方向もしくは内周方向に移動する。トラックエラー検出信号の一部を光学ヘッド移動機構（送りモータ）２０３への駆動電流として供給した場合には、それに合わせて光学ヘッド２０２が徐々に外周方向もしくは内周方向に移動する。

【０２５５】このようにして対物レンズアクチュエータのトラックずれ補正の負担を軽減し、トラックループを安定化出来る。

【０２５６】［１３－４］終了制御

一連の処理が完了し、動作を終了させる場合には以下の手順に従って処理が行われる。

【０２５７】１）制御部２２０から対物レンズアクチュエータ駆動回路２１８に対してトラックループをＯＦＦさせるコマンドが出される。

【０２５８】２）制御部２２０から対物レンズアクチュエータ駆動回路２１８に対してフォーカスループをＯＦＦさせるコマンドが出される。

【０２５９】３）制御部２２０から記録／再生／消去制御波形発生回路２０６に対して半導体レーザ素子の発光を停止させるコマンドが出される。

【０２６０】４）スピンドルモータ駆動回路２１５に対して基準回転数として０を通知する。

【０２６１】［１４］情報記憶媒体への記録信号／再生信号の流れ

［１４－１］情報記憶媒体２０１に記録される信号形式

情報記憶媒体２０１上に記録する信号に対して

◎情報記憶媒体２０１上の欠陥に起因する記録情報エラーの訂正を可能とする

◎再生信号の直流成分を０にして再生処理回路の簡素化を図る

◎情報記憶媒体２０１に対して出来るだけ高密度に情報を記録するとの要求を満足するため図９に示すように情報記録再生部（物理系ブロック）２００では“エラー訂正機能の付加”“記録情報に対する信号変換（信号の変復調）”を行っている。

【０２６２】［１４－２］記録時の信号の流れ

［１４－２－１］ＥＣＣ(Error Correction Code)付加処理

情報記憶媒体２０１に記録したい情報が生信号の形で記録信号ｄとしてデータ入出力インターフェース部３０に入力される。この記録信号ｄはそのまま半導体メモリ２１９に記録され、その後ＥＣＣエンコーディング回路２０８で以下のようにＥＣＣの付加処理を実行する。

【０２６３】以下に積符号を用いたＥＣＣ付加方法の実施例について説明する。

【０２６４】記録信号ｄは半導体メモリ２１９内で１７２Bytes 毎に１行ずつ順次並べ、１９２行で１組のＥＣＣブロックとする。この“行:１７２×列:１９２Bytes”で構成される１組のＥＣＣブロック内の生信号(記録信号ｄ)に対し、１７２Bytesの１行毎に１０Bytes の内符号ＰＩを計算して半導体メモリ２１９内に追加記録する。 さらに Bytes 単位の１列毎に１６Bytes の外符号ＰＯを計算して半導体メモリ２１９内に追加記録する。

【０２６５】情報記憶媒体２０１に記録する実施例としては内符号ＰＩを含めた１２行と外符号ＰＯ分１行の合計２３６６Bytes

（　２３６６＝（１２＋１）×（１７２＋１０））

を単位として情報記憶媒体の１セクター内に記録する。

【０２６６】ＥＣＣエンコーディング回路２０８では内

符号ＰＩと外符号ＰＯの付加が完了すると、半導体メモリ２１９から１セクター分の２３６６Bytes ずつの信号を読み取り、変調回路２０７へ転送する。

【０２６７】［１４－２－２］信号変調

再生信号の直流成分（ ＤＳＶ:Disital Sum Value ）を０に近付け、情報記憶媒体２０１に対して高密度に情報を記録するため、信号形式の変換である信号変調を変調回路２０７内で行う。

【０２６８】元の信号と変調後の信号との間の関係を示す変換テーブルを変調回路２０７と復調回路２１０内部で持っている。ＥＣＣエンコーディング回路２０８から転送された信号を変調方式に従って複数ビット毎に区切り、変換テーブルを参照しながら別の信号（コード）に変換する。

【０２６９】例えば変調方式として８／１６変調（ ＲＬＬ(２,１０)コード）を用いた場合には、変換テーブルが２種類存在し、変調後の直流成分（ ＤＳＶ:Disital SumValue ）が０に近付くように逐一参照用変換テーブルを切り替えている。

【０２７０】［１４－２－３］記録波形発生

情報記憶媒体（光ディスク）２０１に記録マークを記録する場合、一般的には記録方式として

○マーク長記録方式：記録マークの前端位置と後端末位置に“１”が来る。と

○マーク間記録方式：記録マークの中心位置が“１”の位置と一致する。

【０２７１】の２種類存在する。

【０２７２】またマーク長記録を行った場合、長い記録マークを形成する必要が有る。この場合、一定期間記録光量を照射し続けると情報記憶媒体２０１の光反射性記録膜の蓄熱効果により後部のみ幅が広い“雨だれ”形状の記録マークが形成される。この弊害を除去するため、長さの長い記録マークを形成する場合には複数の記録パルスに分割したり、記録波形を階段状に変化させている。

【０２７３】記録／再生／消去制御波形発生回路２０６内では変調回路２０７から送られて来た記録信号に応じて上記のような記録波形を作成し、半導体レーザ駆動回路２０５に伝達している。

【０２７４】［１４－３］再生時の信号の流れ

［１４－３－１］２値化・ＰＬＬ回路

“［１１－１－１］光学ヘッド２０２による信号検出”で記述したように情報記憶媒体（光ディスク）２０１の光反射膜もしくは光反射性記録膜からの反射光量変化を検出して情報記憶媒体２０１上の信号を再生する。アンプ２１３で得られた信号はアナログ波形をしている。２値化回路２１２ではその信号をコンパレーターを用いて“１”と“０”からなる２値のデジタル信号に変換する。

【０２７５】ここから得られた再生信号からＰＬＬ回路２１１で情報再生時の基準信号を取り出している。ＰＬＬ回路２１１は周波数可変の発振器を内蔵している。その発振器から出力されるパルス信号（基準クロック）と２値化回路２１２出力信号間の周波数と位相の比較を行い、その結果を発振器出力にフィードバックしている。

【０２７６】［１４－３－２］信号の復調

変調された信号と復調後の信号との間の関係を示す変換テーブルを復調回路２１０内部で持っている。ＰＬＬ回路２１１で得られた基準クロックに合わせて変換テーブルを参照しながら信号を元の信号に戻す。戻した（復調した）信号は半導体メモリ２１９に記録される。

【０２７７】［１４－３－３］エラー訂正処理

半導体メモリ２１９に保存された信号に対し、内符号ＰＩと外符号ＰＯを用いてエラー訂正回路２０９ではエラー箇所を検出し、エラー箇所のポインタフラグを立てる。

【０２７８】その後、半導体メモリ２１９から信号を読み出しながらエラーポインタフラグに合わせて逐次エラー箇所の信号を訂正し、内符号ＰＩと外符号ＰＯをはずしてデータ入出力インターフェース部３０へ転送する。

【０２７９】ＥＣＣエンコーディング回路２０８から送られて来た信号をデータ入出力インターフェース部３０から再生信号ｃとして出力する。

【０２８０】図１０に上記情報記録再生装置１を用いたパーソナルコンピュータシステム構成を示す。

【０２８１】この場合、上記データ伝送インターフェース部８は情報記録再生装置１、情報再生装置１２２等に設けられるＳＣＳＩ、ＡＴＡＰＩ用のインターフェース回路に対応し、上記外部データ伝送インターフェース部７はＳＣＳＩボード１３８、ＩＤＥコントローラ１２０、ＩＥＥＥ１３９４Ｉ／Ｆボード１３２に対応している。

【０２８２】［１５］一般的なパーソナルコンピュータシステム１５０の内部構造説明

［１５－１］メインＣＰＵ１１１に直接接続されるデータ／アドレスライン

パーソナルコンピュータ１５０内のメインＣＰＵ１１１はメインメモリ１１２との間の情報入出力を直接行うメモリデータライン１１４と、メインメモリ１１２内に記録されている情報のアドレスを指定するメモリアドレスライン１１３を持ち、メインメモリ１１２内にロードされたプログラムに従ってメインＣＰＵ１１１の実行処理が進む。更にメインＣＰＵ１１１はＩ／Ｏデータライン１４６を通して各種コントローラとの情報転送を行うと共に、Ｉ／Ｏアドレスライン１４５のアドレス指定により情報転送先コントローラの指定と転送される情報内容の指定を行っている。

【０２８３】［１５－２］ＣＲＴディスプレイコントロールとキーボードコントロール

ＣＲＴディスプレイ１１６の表示内容制御を行うＬＣＤ

コントローラ１１５はメモリデータライン１１４を介しメインＣＰＵ１１１間の情報交換を行っている。更に高解像度・豊富な表現色を実現するためＣＲＴディスプレイ１１６専用のメモリとしてビデオＲＡＭ１１７を備えている。ＬＣＤコントローラ１１５はメモリデータライン１１４を経由してメインメモリ１１２から直接情報を入力し、ＣＲＴディスプレイ１１６に表示する事も出来る。

【０２８４】キーボード１１９から入力されたテンキー情報はキーボードコントローラ１１８で変換されてＩ／Ｏデータライン１４６を経由してメインＣＰＵ１１１に入力される。

【０２８５】［１５－３］内蔵型ＨＤＤ／情報再生装置の制御系統

パーソナルコンピュータシステム１５０内に内蔵されたＨＤＤ１２１やＣＤ－ＲＯＭドライブ・ＤＶＤ－ＲＯＭドライブなどの光学式の情報再生装置１２２にはＩＤＥインターフェースが使われる場合が多い。ＨＤＤ１２１や情報再生装置１２２からの再生情報、またはＨＤＤ１２１への記録情報はＩＤＥコントローラ１２０を経由してＩ／Ｏデータライン１４６に転送される。

【０２８６】特にブートディスクとしてＨＤＤ１２１を用いた場合にはパーソナルコンピュータシステム１５０起動時にメインＣＰＵ１１１がＨＤＤ１２１にアクセスし、必要な情報がメインメモリ１１２に転送される。

【０２８７】［１５－４］外部とのシリアル／パラレルインターフェース

パーソナルコンピュータシステム１５０の外部機器との情報転送にはシリアルラインとパラレルラインがそれぞれ用意されている。

【０２８８】“セントロ”に代表されるパラレルラインを制御するパラレルＩ／Ｆコントローラ１２３は例えばネットワークを介さずに直接プリンタ１２４やスキャナ１２５を駆動する場合に使われる。スキャナ１２５から転送される情報はパラレルＩ／Ｆコントローラ１２３を経由してＩ／Ｏデータライン１４６に転送される。またＩ／Ｏデータライン１４６上で転送される情報はパラレルＩ／Ｆコントローラ１２３を経由してプリンタ１２４へ転送される。

【０２８９】例えばＣＲＴディスプレイ１１６に表示されているビデオＲＡＭ１１７内の情報やメインメモリ１１２内の特定情報をプリントアウトする場合、これらの情報をメインＣＰＵ１１１を介してＩ／Ｏデータライン１４６に転送した後、パラレルＩ／Ｆコントローラ１２３でプロトコル変換してプリンタ１２４に出力される。

【０２９０】外部に出力されるシリアル情報に関してはＩ／Ｏデータライン１４６で転送された情報がシリアルＩ／Ｆコントローラ１３０でプロトコル変換され、例えばＲＳ－２３２Ｃ信号ｅとして出力される。

【０２９１】［１５－５］機能拡張用バスライン

パーソナルコンピュータシステム１５０は機能拡張用に各種のバスラインを持っている。デスクトップのパーソナルコンピュータではバスラインとしてＰＣＩバス１３３とＥＩＳＡバス１２６を持っている場合が多い。各バスラインはＰＣＩバスコントローラ１４３またはＥＩＳＡバスコントローラ１４４を介してＩ／Ｏデータライン１４６とＩ／Ｏアドレスライン１４５に接続されている。バスラインに接続される各種ボードはＥＩＳＡバス１２６専用ボードとＰＣＩバス１３３専用ボードに分かれている。比較的ＰＣＩバス１３３の方が高速転送に向くため図９ではＰＣＩバス１３３に接続しているボードの数が多くなっているが、それに限らずＥＩＳＡバス１２６専用ボードを使用すれば例えばＬＡＮボード１３９やＳＣＳＩボード１３８をＥＩＳＡバス１２６に接続する事も可能である。

【０２９２】［１５－６］バスライン接続の各種ボードの概略機能説明

◎サウンドブラスターボード１２７：マイク１２８から入力された音声信号はサウンドブラスターボード１２７によりデジタル情報に変換され、ＥＩＳＡバス１２６、Ｉ／Ｏデータライン１４６を経由してメインメモリ１１２やＨＤＤ１２１、情報記録再生装置１に入力され、加工される。

【０２９３】また音楽や音声を聞きたい場合にはＨＤＤ１２１、１４１や情報再生装置１２２、情報記録再生装置１内に記録されているファイル名をユーザが指定する事によりデジタル音源信号がＩ／Ｏデータライン１４６、ＥＩＳＡバス１２６を経由してサウンドブラスターボード１２７に転送され、アナログ信号に変換された後、スピーカー１２９から出力される。

【０２９４】◎専用ＤＳＰ１３７：有る特殊な処理を高速で実行したい場合、その処理専用のＤＳＰ１３７ボードをバスラインに接続する事が出来る。

【０２９５】◎ＳＣＳＩインターフェース：外部記憶装置との間の情報入出力にはＳＣＳＩインターフェースを利用する場合が多い。情報バックアップ用ＭＴ（磁気テープ）１４２、外部据置き型ＨＤＤ１４１、情報記録再生装置１等の外部記憶装置との間で入出力されるＳＣＳＩフォーマット情報をＰＣＩバス１３３またはＥＩＳＡバス１２６に転送するためのプロトコル変換や転送情報フォーマット変換をＳＣＳＩボード１３８内で実行している。

【０２９６】◎情報圧縮・伸長専用ボード：音声、静止画、動画像などマルチメディア情報は情報圧縮してＨＤＤ１２１、１４１や情報記録再生装置１（情報再生装置１２２）に記録される。

【０２９７】ＨＤＤ１２１、１４１や情報記録再生装置１、情報再生装置１２２に記録されている情報を伸長してＣＲＴディスプレイ１１６に表示したり、スピーカー１２９に鳴らす。またマイク１２８から入力された音声

信号などを情報圧縮してＨＤＤ１２１、１４１や情報記録再生装置１に記録する。

【０２９８】この情報の圧縮・伸長機能を各種専用ボードが受け持っている。音楽・音声信号の圧縮・伸長を音声符号化・復号化ボード１３６で行い、動画像（ビデオ映像）の圧縮・伸長をＭＰＥＧボード１３４で行い、サブピクチャー（副映像）の圧縮・伸長をサブピクチャーランレングス用ボード１３５で行っている。

【０２９９】［１６］パーソナルコンピュータシステム１５０の外部ネットワークとの接続

［１６－１］電話回線を用いたネットワーク接続

電話回線ｆを経由して外部に情報転送したい場合には、モデム１３１を用いる。すなわち希望の相手先へ電話接続するには図示して無いがＮＣＵ（Network Control Unit）が電話回線ｆを介して電話交換機に相手先電話番号を伝達する。電話回線が接続されると、シリアルＩ／Ｆコントローラ１３０がＩ／Ｏデータライン１４６上の情報に対して転送情報フォーマット変換とプロトコル変換を行い、その結果得られるデジタル信号のＲＳ－２３２Ｃ信号をモデム１３１でアナログ信号に変換して電話回線ｆに転送される。

【０３００】［１６－２］ＩＥＥＥ１３９４を用いたネットワーク接続

音声、静止画、動画像などマルチメディア情報を外部装置（図示して無い）へ転送する場合にはＩＥＥＥ１３９４インターフェースが適している。

【０３０１】動画や音声では一定時間内に必要な情報を送り切れないと画像の動きがギクシャクしたり、音声が途切れたりする。その問題を解決するためＩＥＥＥ１３９４では１２５μｓ毎にデータ転送が完了する isochronous 転送方式を採用している。ＩＥＥＥ１３９４ではこの isochronous 転送と通常の非同期転送の混在も許しているが、１サイクルの非同期転送時間は最大６３．５μｓと上限が決められている。この非同期転送時間が長過ぎると isochronous 転送を保証できなくなるためで有る。ＩＥＥＥ１３９４ではＳＣＳＩのコマンド（命令セット）をそのまま使用する事が出来る。

【０３０２】ＰＣＩバス１３３を伝わって来た情報に対し、isochronous 転送用の情報フォーマット変換やプロトコル変換、ノード設定のようなトポロジーの自動設定などの処理をＩＥＥＥ１３９４Ｉ／Ｆボード１３２が行っている。

【０３０３】このようにパーソナルコンピュータシステム１５０内で持っている情報をＩＥＥＥ１３９４信号ｇとして外部に転送するだけで無く、同様に外部から送られて来るＩＥＥＥ１３９４信号ｇを変換してＰＣＩバス１３３に転送する働きもＩＥＥＥ１３９４Ｉ／Ｆボード１３２は持っている。

【０３０４】［１６－３］ＬＡＮを用いたネットワーク接続

企業内や官庁・学校など特定地域内のローカルエリア情報通信には図示して無いがＬＡＮケーブルを媒体としてＬＡＮ信号ｈの入出力を行っている。

【０３０５】ＬＡＮを用いた通信のプロトコルとしてＴＣＰ／ＩＰ、ＮｅｔＢＥＵＩなどが存在し、各種プロトコルに応じて独自のデータパケット構造（情報フォーマット構造）を持つ。ＰＣＩバス１３３上で転送される情報に対する情報フォーマット変換や各種プロトコルに応じた外部との通信手続き処理などをＬＡＮボード１３９が行う。

【０３０６】例としてＨＤＤ１２１内に記録して有る特定ファイル情報をＬＡＮ信号ｈに変換して外部のパーソナルコンピュータやＥＷＳ、あるいはネットワークサーバー（図示して無い）に転送する場合の手続きと情報転送経路について説明する。ＩＤＥコントローラ１２０の制御によりＨＤＤ１２１内に記録されているファイルディレクトリを出力させ、その結果のファイルリストをメインＣＰＵ１１１がメインメモリ１１２に記録すると共に、ＣＲＴディスプレイ１１６に表示させる。ユーザが転送したいファイル名をキーボード１１９入力するとその内容がキーボードコントローラ１１８を介してメインＣＰＵ１１１に認識される。メインＣＰＵ１１１がＩＤＥコントローラ１２０に転送するファイル名を通知すると、ＨＤＤが内部の情報記録場所を判定してアクセスし、再生情報がＩＤＥコントローラ１２０を経由してＩ／Ｏデータライン１４６に転送される。Ｉ／Ｏデータライン１４６からＰＣＩバスコントローラ１４３にファイル情報が入力された後、ＰＣＩバス１３３を経由してＬＡＮボード１３９へ転送される。ＬＡＮボード１３９では一連の通信手続きにより転送先とセッションを張った後、ＰＣＩバス１３３からファイル情報を入力し、伝送するプロトコルに従ったデータパケット構造に変換後ＬＡＮ信号ｈとして外部へ転送する。

【０３０７】［１７］情報再生装置または情報記録再生装置(光ディスク装置)からの情報転送

［１７－１］標準的インターフェースと情報転送経路

ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどの再生専用光ディスク装置である情報再生装置１２２やＤＶＤ－ＲＡＭ、ＰＤ、ＭＯなどの記録再生可能な光ディスクである情報記録再生装置１をパーソナルコンピュータシステム１５０内に組み込んで使用する場合、標準的なインターフェースとして“ＩＤＥ”“ＳＣＳＩ”“ＩＥＥＥ１３９４”などが存在する。

【０３０８】一般的にはＰＣＩバスコントローラ１４３やＥＩＳＡバスコントローラ１４４は内部にＤＭＡを持っている。ＤＭＡの制御によりメインＣＰＵ１１１を介在させる事無く各ブロック間で直接情報を転送する事が出来る。

【０３０９】例えば情報記録再生装置１の情報をＭＰＥＧボード１３４に転送する場合メインＣＰＵ１１１から

の処理はＰＣＩバスコントローラ１４３へ転送命令を与えるだけで、情報転送管理はＰＣＩバスコントローラ内のＤＭＡに任せる。その結果、実際の情報転送時にはメインＣＰＵは情報転送処理に悩殺される事無く並列して他の処理を実行できる。

【０３１０】同様に情報再生装置１２２内に記録されている情報をＨＤＤ１４１へ転送する場合もメインＣＰＵ１１１はＰＣＩバスコントローラ１４３またはＩＤＥコントローラ１２０へ転送命令を出すだけで、後の転送処理管理をＰＣＩバスコントローラ１４３内のＤＭＡまたはＩＤＥコントローラ１２０内のＤＭＡに任せている。

【０３１１】［１７－２］認証（ authentication ）機能

情報記録再生装置１もしくは情報再生装置１２２に関する情報転送処理には上述したようにＰＣＩバスコントローラ１４３内のＤＭＡ、ＥＩＳＡバスコントローラ１４４内のＤＭＡまたはＩＤＥコントローラ１２０内のＤＭＡが管理を行っているが、実際の転送処理自体は情報記録再生装置１もしくは情報再生装置１２２が持つ認証（ authentication ）機能部が実際の転送処理を実行している。

【０３１２】ＤＶＤビデオ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲなどのＤＶＤシステムではビデオ、オーディオのビットストリームは ＭＰＥＧ２ Program stream フォーマットで記録されており、オーディオストリーム、ビデオストリーム、サブピクチャーストリーム、プライベートストリームなどが混在して記録されている。情報記録再生装置１は情報の再生時にプログラムストリーム（ Program stream ）からオーディオストリーム、ビデオストリーム、サブピクチャーストリーム、プライベートストリームなどを分離抽出し、メインＣＰＵ１１１を介在させる事無くＰＣＩバス１３３を介して直接音声符号化復号化ボード１３６、ＭＰＥＧボード１３４あるいはサブピクチャーランレングス用ボード１３５に転送する。

【０３１３】同様に情報再生装置１２２もそこから再生されるプログラムストリーム（ Program stream ）を各種のストリーム情報に分離抽出し、個々のストリーム情報をＩ／Ｏデータライン１４６、ＰＣＩバス１３３を経由して直接（メインＣＰＵ１１１を介在させる事無く）音声符号化復号化ボード１３６、ＭＰＥＧボード１３４あるいはサブピクチャーランレングス用ボード１３５に転送する。

【０３１４】情報記録再生装置１や情報再生装置１２２と同様音声符号化復号化ボード１３６、ＭＰＥＧボード１３４あるいはサブピクチャーランレングス用ボード１３５自体にも内部に認証（ authentication ）機能を持っている。情報転送に先立ち、ＰＣＩバス１３３（およびＩ／Ｏデータライン１４６）を介して情報記録再生装置１や情報再生装置１２２と音声符号化復号化ボード１３６、ＭＰＥＧボード１３４、サブピクチャーランレングス用ボード１３５間で互いに認証し合う。相互認証が完了すると情報記録再生装置１や情報再生装置１２２で再生されたビデオストリーム情報はＭＰＥＧボード１３４だけに情報転送する。同様にオーディオストリーム情報は音声符号化復号化ボード１３６のみに転送される。また静止画ストリームはサブピクチャーランレングス用ボード１３５へ、プライベートストリームやテキスト情報はメインＣＰＵ１１１へ送られる。

【０３１５】次に、図１０に示すＭＰＥＧボード１３４（認証相手２）と情報記録再生装置１とのデータのやり取りについて、図１１を用いて説明する。この場合、ＭＰＥＧボード１３４と情報記録再生装置１との間に介在しているＰＣＩバス１３３とＳＣＳＩボードについては説明を省略する。この場合、ＭＰＥＧボード１３４にも認証機能部９を有し、認証情報記憶部２４としては縦１列分の記憶がなされるようになっている。

【０３１６】すなわち、情報記録再生装置１からのＡＧＩＤ、設定エリア情報、ストリームＩＤからなるレポートキーコマンドがＭＰＥＧボード１３４に出力される(1)。

【０３１７】ＭＰＥＧボード１３４は供給されたＡＧＩＤ、設定エリア情報、ストリームＩＤ（サブストリームＩＤ）に基づいてあらかじめ記憶されているストリームキーとエリアキーとを読出し、この読出したストリームキーとエリアキーとからなる合成キーで暗号化したチャレンジキーＡを作成し、この暗号化されたチャレンジキーＡを含むセンドキーコマンドを情報記録再生装置１に出力する(2)。

【０３１８】情報記録再生装置１は、供給されたチャレンジキーＡに基づいて暗号化された暗号化キー１を生成し、この暗号化された暗号化キー１からなるレポートキーコマンドがＭＰＥＧボード１３４に出力される(3)。ついで、情報記録再生装置１は、あらかじめ記憶されているストリームキーとエリアキーとを読出し、この読出したストリームキーとエリアキーとからなる合成キーで暗号化したチャレンジキーＢを生成し、チャレンジキーＢを含むレポートキーコマンドがＭＰＥＧボード１３４に出力される(4)。

【０３１９】ＭＰＥＧボード１３４は供給されたチャレンジキーＢに基づいて暗号化された暗号化キー２を含むセンドキーコマンドを情報記録再生装置１に出力する(5)。

【０３２０】情報記録再生装置１は、供給された暗号化されている暗号化キー２から解読した暗号化キー２と上記作成した暗号化キー１とによりバスキーを作成する(6)。

【０３２１】また、ＭＰＥＧボード１３４は供給された暗号化されている暗号化キー１から解読した暗号化キー１と上記作成した暗号化キー２とによりバスキーを作成する(6)。

【０３２２】上記例として(3)（4）の動作について詳細に説明する。

【０３２３】たとえば、相手から暗号化されたチャレンジキーが送られてきた時、つまりＭＰＥＧボード１３４から外部データ伝送インターフェース部７、データ伝送インターフェース部８を介して供給されるチャレンジキーを外部伝送データ記憶部２５に記憶する。

【０３２４】ついで、暗号化部／復号化部／時変情報発生部２３内のランダム信号発生器１０４の出力信号を暗号化キー１とし、シフトレジスタ１０９ａからｄの出力ｉ５を入出力信号切り替え制御器１０６、バスライン２６を介して認証情報記憶部２４の自分が発行する暗号化キー１情報５５に記憶させる。

【０３２５】これに続くランダム信号発生器１０４の一単位の数字を時変情報として、つまりシフトレジスタ１０９ａからｄの出力ｉ５を入出力信号切り替え制御器１０６、バスライン２６を介して認証情報記憶部２４のランダム信号発生器１０４で作られるタイムリーな時変情報３９に登録しておく。

【０３２６】チャレンジキーの解読まず、認証情報記憶部２４の情報ａ対応のストリームキー情報３１が読み出されてバスライン２６、入出力信号切り替え制御器１０６を介してセレクタ１０７に出力され、シフトレジスタ１０９ａに送られる。

【０３２７】ストリームキー情報３１が送り終り、第１エリアキー情報３５が読み出されてバスライン２６、入出力信号切り替え制御器１０６を介してセレクタ１０７に出力され、シフトレジスタ１０９ａに送られる。

【０３２８】この結果、シフトレジスタ１０９ａ、ｂにストリームキーが入り、シフトレジスタ１０９ｃ、ｄに第１エリアキーが入る。

【０３２９】ここで合成キーの作成完了し、シフトレジスタ１０９ａからｄの出力ｉ５として信号合成器１０５へ出力される。

【０３３０】次に、外部伝送データ記憶部２５に記憶されていた暗号化されたチャレンジキーがバスライン２６、入出力信号切り替え制御器１０６を介して入力ｉ２として信号合成器１０５へ出力される。

【０３３１】信号合成器１０５は、供給される合成キーにより暗号化されたチャレンジキーが復号されたものがシフトレジスタ１１０ｄ～ａへ出力される。

【０３３２】外部伝送データ記憶部２５からの５６ビットのチャレンジキー送信終了後、シフトレジスタ１１０ｄ～ａに復号されたチャレンジキーがすべて入る。

【０３３３】この後、シフトレジスタ１１０ｄ～ａから出力されるチャレンジキーが入出力信号切り替え制御器１０６、バスライン２６を介して認証情報記憶部２４の相手が発行するチャレンジキー情報４５に記憶される。

【０３３４】この相手が発行するチャレンジキー情報４５を利用して自分が発行する暗号化キー１情報５５を暗号化する。

【０３３５】自分が発行するチャレンジキー情報５１を認証情報記憶部２４から読み出して、バスライン２６、入出力信号切り替え制御器１０６を介してセレクタ１０７に出力され、シフトレジスタ１０９ａに送られる。

【０３３６】この結果、シフトレジスタ１０９ａからｄに自分が発行するチャレンジキー情報５１が入る。このチャレンジキー情報５１がシフトレジスタ１０９ａからｄの出力ｉ５として信号合成器１０５へ出力される。

【０３３７】次に、自分が発行する暗号化キー１情報５５を認証情報記憶部２４から読み出して、バスライン２６、入出力信号切り替え制御器１０６を介して入力ｉ２として信号合成器１０５へ出力される。

【０３３８】信号合成器１０５は、供給される暗号化キー１情報５５をチャレンジキー情報５１により暗号化し、この暗号化された暗号化キー１がシフトレジスタ１１０ｄ～ａへ出力される。

【０３３９】この後、シフトレジスタ１１０ｄ～ａから出力される暗号化された暗号化キー１が入出力信号切り替え制御器１０６、バスライン２６を介して外部伝送データ記憶部２５に記憶される。

【０３４０】この外部伝送データ記憶部２５に記憶された暗号化された暗号化キー１にレポートコマンド等を付与してデータ伝送インターフェース部８、外部データ伝送インターフェース部７を介してＭＰＥＧボード１３４へ送信される。

【０３４１】次に、認証情報記憶部２４のランダム信号発生器１０４で作られるタイムリーな時変情報３９が読み出されてバスライン２６、入出力信号切り替え制御器１０６を介してセレクタ１０７に出力され、シフトレジスタ１０９ａからｄに送られる。

【０３４２】すべての時変情報３９が、シフトレジスタ１０９ａからｄに入ったらセレクタ１０７を閉じる。これにより、ランダム信号発生器１０４の時変キーがランダム処理される。

【０３４３】バスキーの作成　暗号化キー１、暗号化キー２で作る。

【０３４４】すなわち、自分が発行する暗号化キー１情報５５が認証情報記憶部２４から読み出されて、バスライン２６、入出力信号切り替え制御器１０６を介してセレクタ１０７に出力され、シフトレジスタ１０９ａに送られる。

【０３４５】この結果、シフトレジスタ１０９ａからｄに自分が発行する暗号化キー１情報５５が入る。この暗号化キー１情報５５がシフトレジスタ１０９ａからｄの出力ｉ５として信号合成器１０５へ出力される。

【０３４６】また、相手が発行する暗号化キー２情報６０が認証情報記憶部２４から読み出されて、バスライン２６、入出力信号切り替え制御器１０６を介して入力ｉ２として信号合成器１０５へ出力される。

【０３４７】信号合成器１０５は、供給される暗号化キー１情報５５と暗号化キー２情報６０とが合成されてバスキーが生成され、シフトレジスタ１０９ａからｄの出力ｉ５を入出力信号切り替え制御器１０６、バスライン２６を介して認証情報記憶部２４のバスキー情報６５に記憶させる。

【０３４８】上記したように、メインＣＰＵ１１１が介在せずに、情報記録再生装置１と各処理ボード１３４、１３５、１３６とのデータの伝送を行えることができ、メインＣＰＵ１１１の負担を軽減でき、情報伝送期間中にメインＣＰＵ１１１が他の処理を行うことができる。

【０３４９】また、シフトレジスタ１０９ａ、からｄを用いたランダム信号発生器１０４を用いることにより、非常に簡単な構成で暗号化／復号化（解読）を行える。

【０３５０】また、暗証機能部９内の時変情報発生部２３で暗号鍵を発行するため、公開鍵を管理する第３者を置くことなく容易に相互認証可能、つまり第３者の介在や第３者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【０３５１】また、暗証機能部９内で作成した暗号鍵を認証相手から送られた暗号鍵で暗号化して認証相手に伝送することにより、公開鍵方式を用いるよりも遙かに暗号化の信頼性が高く、情報漏洩を防げる。

【０３５２】また、情報記録媒体からの情報に付与されている情報の種類を示す情報（ストリームＩＤ）から認証相手を同定することにより、各認証相手に対して認証後、各認証相手にパラレルに情報を配信（送信）でき、この結果、各認証相手の負担が相対的に軽減すると共に情報記録媒体から情報再生を開始してから短時間で（ＴＶ）画面上に表示でき、タイムラグを最小に抑えることができる。

【０３５３】また、送信したい情報から認証相手を探すことができ、認証候補相手に対して情報を提供し、該当相手から回答してもらい、その回答結果に基付き相互認証作業に入るという方式により、比較的簡単な方法で認証相手を探すことができる。

【０３５４】また、認証機能部内に暗号化情報記憶用メモリを持たせることにより、メモリと独自のクロックを持つことにより情報を整理することができ、暗号化情報を認証機能部９独自のクロックで外部伝送データ記憶部２５に事前に記録するため、データ伝送インターフェース部８は伝送回線の都合に応じて最適なタイミングで外部伝送データ記憶部２５への情報の記録／再生処理を行うことができ、外部との間で送受信する暗号化情報を外部伝送データ記憶部２５に一時保管し、更に内部に持つ独自のクロックに従って暗号化情報を独立して作成することにより、プロトコル変換時の適応性、外部通信回線混雑状況に対する柔軟性を向上させている。

【０３５５】また、エリアキー情報とストリームキー情報を認証情報記憶部２４に事前に記憶しておき、その情報を認証処理に利用することにより、認証局（ＣＡセンタ）などの第３者の介在や第３者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【０３５６】また、サーバから情報の配送・収集先のクライアント（のＩＰアドレスや電話番号）と配送・収集する情報内容を通知するだけで後の処理を情報記録再生装置１に任せるため、情報伝送中メインＣＰＵ１１１に負担をかけることがなく、情報伝送中もメインＣＰＵ１１１が他の処理をできるのでシステムとしての高速処理を可能とし、さらにコンピュータと情報再生装置間はネットワーク通信で情報の入出力を行うためコンピュータに対して情報再生装置を遠隔地に配置でき、この結果小さなスペースにコンピュータを配置することが可能となる。。

【０３５７】また、情報再生装置が通信機能を持っているので、小型ノートＰＣなどのＰＣＭＣＩＡカードスロットが１個しかない小型ＰＣでも通信用ＬＡＮカードかモデムカードを利用すれば通信しながら情報再生装置間で情報の入出力処理が可能となる。さらに情報再生装置に認証機能を持ち暗号化情報を送れるので通信経路途中での情報コピー、情報漏洩の心配が無い。

【０３５８】さらに、通信機能部を有しただけでなく、認証機能部が通信機能部の通信機能を用いて認証相手との間で相互認証を行い、暗号化情報を伝送することにより、ネットワーク伝送経路途中での情報のコピーによる情報漏洩防止、セキュリティー確保が可能となる。

【０３５９】また、メモリに複数相手との認証履歴を記憶しておくことにより、時分割処理方法を利用して複数の認証相手に対して同時に認証処理と暗号化情報の伝送を可能とし、認証のため長時間待つ認証相手が無くなり、かつ高速で同時に複数の認証相手との認証処理を実行できる。

【０３６０】また、１個のランダム信号発生器１０４を用いて暗号鍵の発行と、情報の暗号化と、暗号化された情報の復号化（解読）の兼用処理を行え、信号合成器１０５を用いて暗号鍵の発行と、情報の暗号化と、暗号化された情報の復号化（解読）の兼用処理を行えるようにしたので、機能兼用化により回路の簡素化と低価格化が図れる。

【０３６１】また、パソコン内の各ボード間で認証処理を実施させることができる。

【０３６２】

【発明の効果】以上詳述したように、この発明によれば、メインの制御部が介在せずに、情報再生装置と各処理ボードとのデータの伝送を行えることができ、メインの制御部の負担を軽減でき、情報伝送期間中にメインの制御部が他の処理を行うことができる。

【０３６３】また、この発明によれば、非常に簡単な構成で暗号化／復号化（解読）を行える。

【０３６４】また、この発明によれば、公開鍵を管理する第３者を置くことなく容易に相互認証可能、つまり第３者の介在や第３者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【０３６５】また、この発明によれば、伝送し合った暗号鍵で他方の暗号鍵を更に暗号化することにより、公開鍵方式を用いるよりも遙かに暗号化の信頼性が高く、情報漏洩を防げる。

【０３６６】また、この発明によれば、情報記録媒体からの情報に付与されている情報の種類を示す情報（ストリームＩＤ）から認証相手を同定することにより、各認証相手に対して認証後、各認証相手にパラレルに情報を配信（送信）でき、この結果、各認証相手の負担が相対的に軽減すると共に情報記録媒体から情報再生を開始してから短時間で（ＴＶ）画面上に表示でき、タイムラグを最小に抑えることができる。

【０３６７】また、この発明によれば、送信したい情報から認証相手を探すことができ、認証候補相手に対して情報を提供し、該当相手から回答してもらい、その回答結果に基付き相互認証作業に入るという方式により、比較的簡単な方法で認証相手を探すことができる。

【０３６８】また、この発明によれば、認証機能部内に暗号化情報記憶用メモリを持たせることにより、メモリと独自のクロックを持つことにより情報を整理することができ、暗号化情報を認証機能部独自のクロックで外部伝送データ記憶部に事前に記録するため、データ伝送インターフェース部は伝送回線の都合に応じて最適なタイミングで外部伝送データ記憶部への情報の記録／再生処理を行うことができ、外部との間で送受信する暗号化情報を外部伝送データ記憶部に一時保管し、更に内部に持つ独自のクロックに従って暗号化情報を独立して作成することにより、プロトコル変換時の適応性、外部通信回線混雑状況に対する柔軟性を向上させている。

【０３６９】また、この発明によれば、エリアキーとストリームキーを認証情報記憶部に事前に記憶しておき、その情報を認証処理に利用することにより、認証局（ＣＡセンタ）などの第３者の介在や第３者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【０３７０】また、この発明によれば、サーバから情報の配送・収集先のクライアント（のＩＰアドレスや電話番号）と配送・収集する情報内容を通知するだけで後の処理を情報再生装置に任せるため、情報伝送中メインＣＰＵに負担をかけることがなく、情報伝送中もメインＣＰＵが他の処理をできるのでシステムとしての高速処理を可能とし、さらにコンピュータと情報再生装置間はネットワーク通信で情報の入出力を行うためコンピュータに対して情報再生装置を遠隔地に配置でき、この結果小さなスペースにコンピュータを配置することが可能となる。。

【０３７１】また、この発明によれば、情報再生装置が通信機能を持っているので、小型ノートＰＣなどのＰＣＭＣＩＡカードスロットが１個しかない小型ＰＣでも通信用ＬＡＮカードかモデムカードを利用すれば通信しながら情報再生装置間で情報の入出力処理が可能となる。さらに情報再生装置に認証機能を持ち暗号化情報を送れるので通信経路途中での情報コピー、情報漏洩の心配が無い。

【０３７２】さらに、通信機能部を有しただけでなく、認証機能部が通信機能部の通信機能を用いて認証相手との間で相互認証を行い、暗号化情報を伝送することにより、ネットワーク伝送経路途中での情報のコピーによる情報漏洩防止、セキュリティー確保が可能となる。

【０３７３】また、この発明によれば、メモリに複数相手との認証履歴を記憶しておくことにより、時分割処理方法を利用して複数の認証相手に対して同時に認証処理と暗号化情報の伝送を可能とし、認証のため長時間待つ認証相手が無くなり、かつ高速で同時に複数の認証相手との認証処理を実行できる。

【０３７４】また、この発明によれば、１個のランダム信号発生器を用いて暗号鍵の発行と、情報の暗号化と、暗号化された情報の復号化（解読）の兼用処理を行えるようにしたので、機能兼用化により回路の簡素化と低価格化が図れる。

【０３７５】また、この発明によれば、パソコン内の各ボード間で認証処理を実施させることができる。

【図面の簡単な説明】

【図１】図１は、この発明の実施の形態に係る認証機能を有する情報記録再生装置の構成を説明するブロック図である。

【図２】図２は、認証機能部の内部構造とそれに接続される周辺機器との関係を示す図である。

【図３】図３は、情報記録媒体に記録されているＶＯＢＵの内部構造説明図である。

【図４】図４は、パックの内部構成を示す図である。

【図５】図５は、認証作業手順を説明するためのフローチャートである。

【図６】図６は、認証情報記憶部内に記憶される履歴情報内容を示す図である。

【図７】図７は、認証処理制御部の構成を説明するブロック図である。

【図８】図８は、暗号化部／復号化部／時変情報発生部の構成を説明するブロック図である。

【図９】図９は、情報記録再生装置内の情報記録再生部の構成を説明するブロック図である。

【図１０】図１０は、パーソナルコンピュータシステムの構成を説明するブロック図である。

【図１１】図１１は、ＭＰＥＧボードと情報記録再生装置とのデータのやり取りを説明するための図である。

【符号の説明】

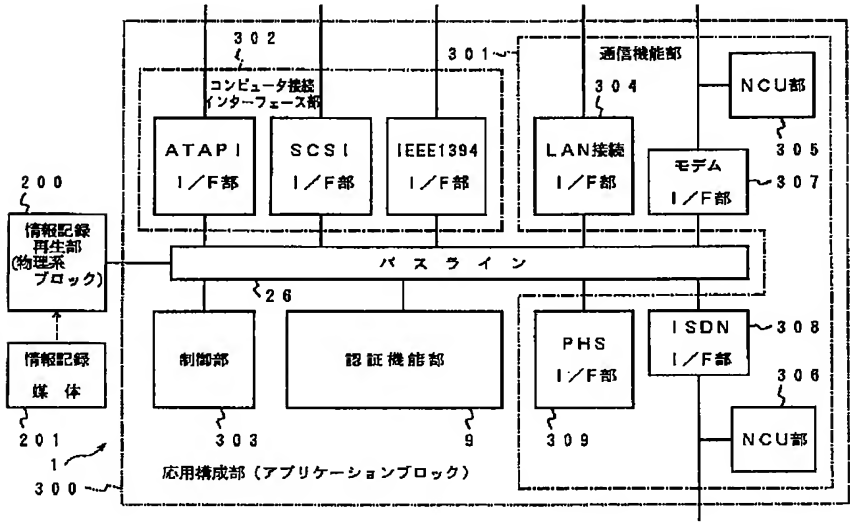
57

1…情報記録再生装置
2～5…認証相手
6、7…外部データ伝送インターフェース部
8…データ伝送インタフェース部
9…認証機能部
１０ａ…ａパック
１０ｂ…ｂパック
１０ｃ…ｃパック
１０ｄ…ｄパック
１１…パックヘッダ
１２…パケット
１３…パケットヘッダ
１４…伝達される情報内容
２１…基準クロック発生部
２２…認証処理制御部
２３…暗号化部／復号化部／時変情報発生部
２４…認証情報記憶部
２５…外部伝送データ記憶部

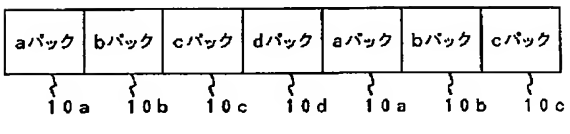
58

＊２６…バスライン
３０…データ入出力インターフェース部
１１１…メインＣＰＵ
１２０…ＩＤＥコントローラ
１２２…情報再生装置
１２７…サウンドブラスターボード
１３０…シリアルＩ／Ｆコントローラ
１３１…モデム
１３２…ＩＥＥＥ１３９４Ｉ／Ｆボード
１３４…ＭＰＥＧボード
１３５…サブピクチャーランレングス用ボード
１３６…音声符号化復号化ボード
１３８…ＳＣＳＩボード
１３９…ＬＡＮボード
１５０…パーソナルコンピュータ
２００…情報記録再生部（物理ブロック）
２０１…情報記録媒体
＊

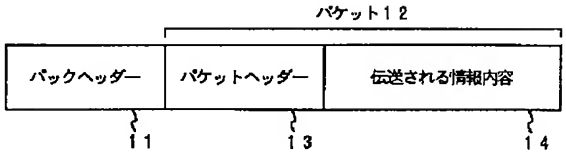
【図１】



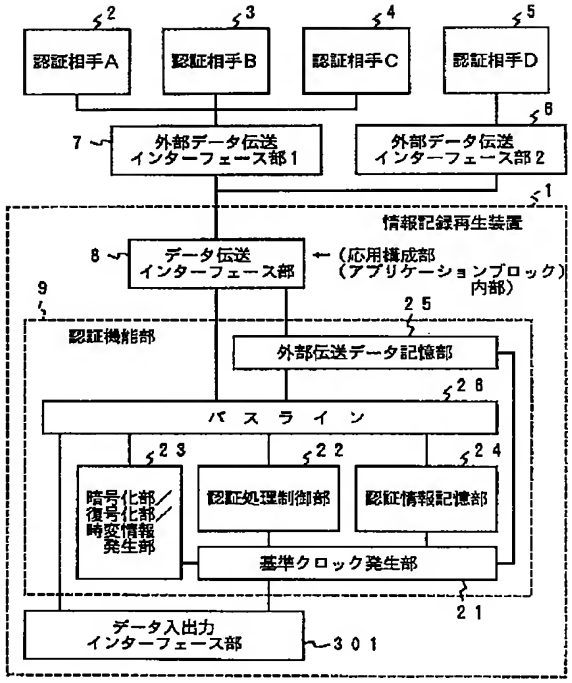
【図３】



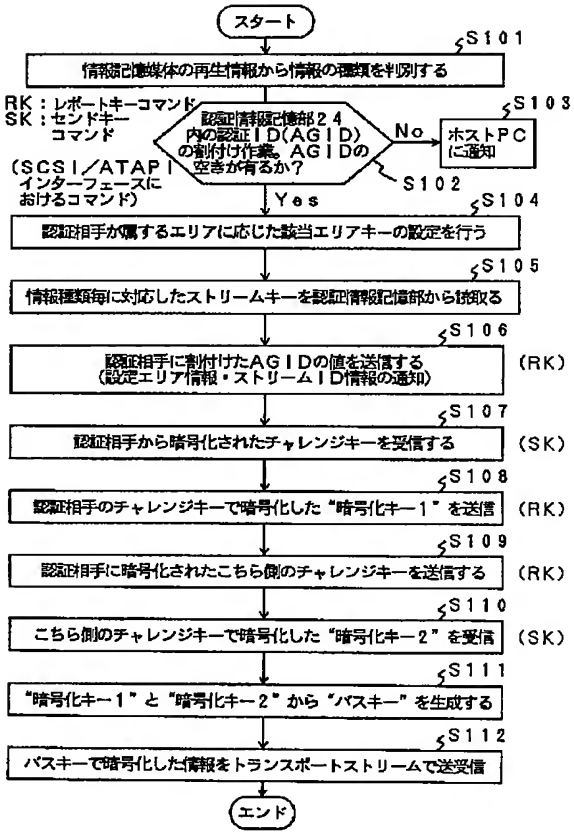
【図４】



【図２】



【図５】

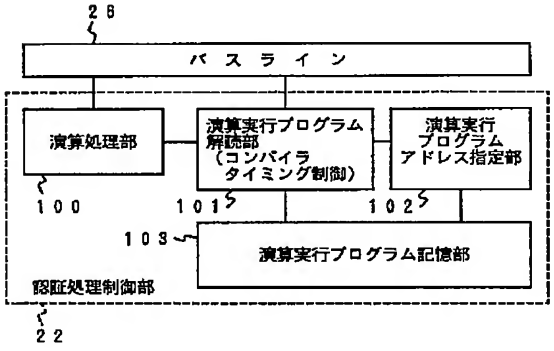


【図６】

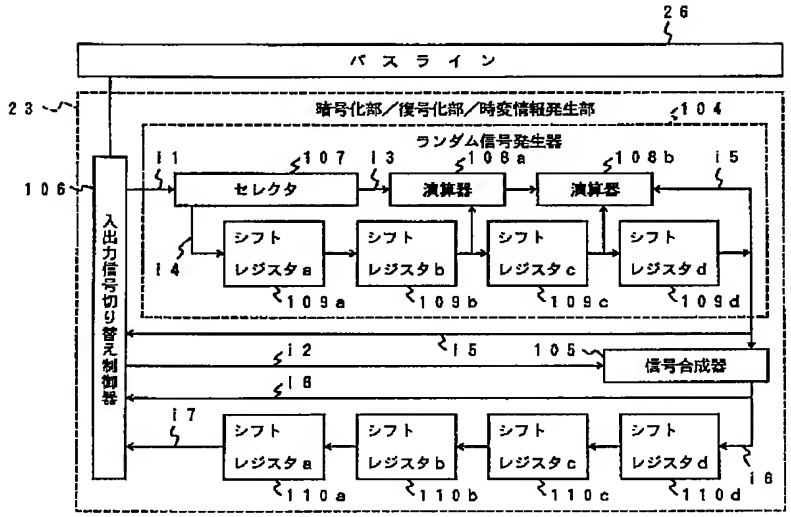
情報a対応のストリームキー情報 31	情報b対応のストリームキー情報 32	情報c対応のストリームキー情報 33	情報d対応のストリームキー情報 34
第1エリアキー情報 35	第2エリアキー情報 36	第3エリアキー情報 37	第4エリアキー情報 38
ランダム信号発生器で作られるタイムリーな時変情報 39			
AGID番号(AGID=0) 40	AGID番号(AGID=1) 41	AGID番号(AGID=2) 42	AGID番号(AGID=3) 43
相手が発行するチャレンジキー情報(AGID=0) 45	相手が発行するチャレンジキー情報(AGID=1) 46	相手が発行するチャレンジキー情報(AGID=2) 47	相手が発行するチャレンジキー情報(AGID=3) 48
自分が発行するチャレンジキー情報(AGID=0) 51	自分が発行するチャレンジキー情報(AGID=1) 52	自分が発行するチャレンジキー情報(AGID=2) 53	自分が発行するチャレンジキー情報(AGID=3) 54
自分が発行する暗号化キー１情報(AGID=0) 55	自分が発行する暗号化キー１情報(AGID=1) 56	自分が発行する暗号化キー１情報(AGID=2) 57	自分が発行する暗号化キー１情報(AGID=3) 58
相手が発行する暗号化キー２情報(AGID=0) 60	相手が発行する暗号化キー２情報(AGID=1) 61	相手が発行する暗号化キー２情報(AGID=2) 62	相手が発行する暗号化キー２情報(AGID=3) 63
バスキー情報(AGID=0) 65	バスキー情報(AGID=1) 66	バスキー情報(AGID=2) 67	バスキー情報(AGID=3) 68
AGID送信完了情報(AGID=0) 70	AGID送信完了情報(AGID=1) 71	AGID送信完了情報(AGID=2) 72	AGID送信完了情報(AGID=3) 73
チャレンジキー受信完了情報(AGID=0) 75	チャレンジキー受信完了情報(AGID=1) 76	チャレンジキー受信完了情報(AGID=2) 77	チャレンジキー受信完了情報(AGID=3) 78
暗号化キー１送信完了情報(AGID=0) 80	暗号化キー１送信完了情報(AGID=1) 81	暗号化キー１送信完了情報(AGID=2) 82	暗号化キー１送信完了情報(AGID=3) 83
チャレンジキー送信完了情報(AGID=0) 85	チャレンジキー送信完了情報(AGID=1) 86	チャレンジキー送信完了情報(AGID=2) 87	チャレンジキー送信完了情報(AGID=3) 88
暗号化キー２受信完了情報(AGID=0) 90	暗号化キー２受信完了情報(AGID=1) 91	暗号化キー２受信完了情報(AGID=2) 92	暗号化キー２受信完了情報(AGID=3) 93

24

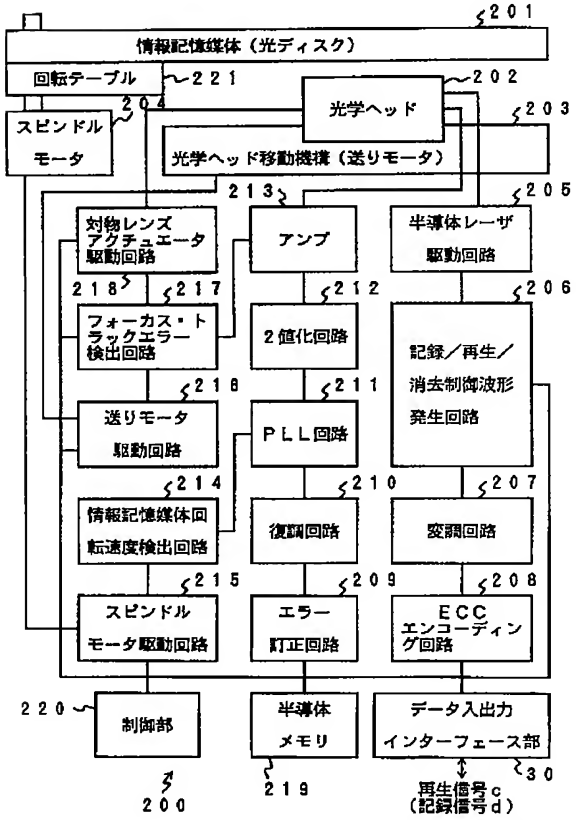
【図７】



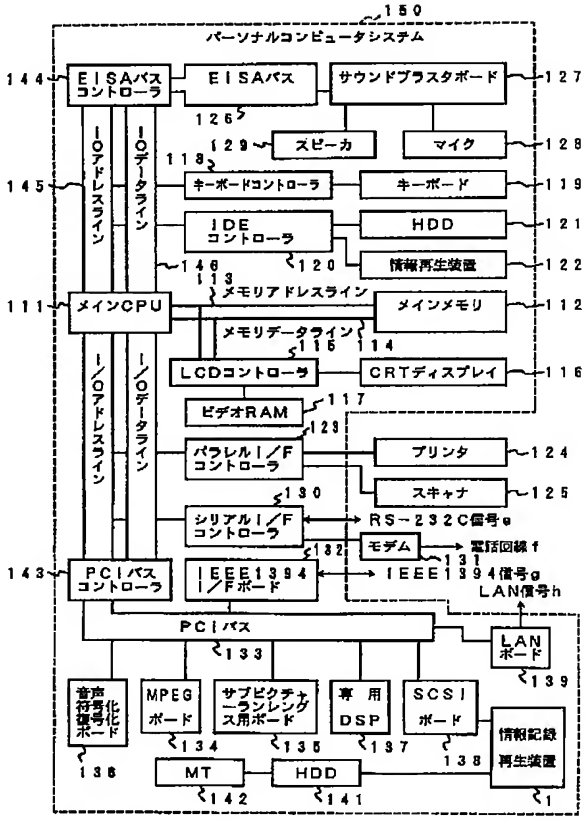
【図８】


２６
バスライン
２３
暗号化部／復号化部／時変情報発生部
１０４
ランダム信号発生器
１０６
入出力信号切り替え制御器
ｉ１
１０７
ｉ３
１０８ａ
１０８ｂ
ｉ５
セレクタ
演算器
演算器
ｉ４
シフトレジスタａ
シフトレジスタｂ
シフトレジスタｃ
シフトレジスタｄ
１０９ａ
１０９ｂ
１０９ｃ
１０９ｄ
ｉ２
１５
１０５
信号合成器
ｉ８
ｉ７
シフトレジスタａ
シフトレジスタｂ
シフトレジスタｃ
シフトレジスタｄ
ｉ６
１１０ａ
１１０ｂ
１１０ｃ
１１０ｄ

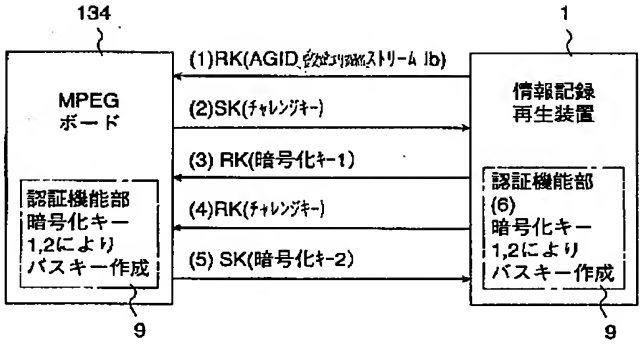
【図９】


２０１
情報記憶媒体（光ディスク）
回転テーブル
２２１
２０２
光学ヘッド
２０４
スピンドルモータ
２０３
光学ヘッド移動機構（送りモータ）
２１３
２０５
対物レンズアクチュエータ駆動回路
アンプ
半導体レーザ駆動回路
２１８
２１７
２１２
２０６
フォーカス・トラックエラー検出回路
２値化回路
記録／再生／消去制御波形発生回路
２１６
２１１
送りモータ駆動回路
ＰＬＬ回路
２１４
２１０
２０７
情報記憶媒体回転速度検出回路
復調回路
変調回路
２１５
２０９
２０８
スピンドルモータ駆動回路
エラー訂正回路
ＥＣＣエンコーディング回路
２２０
制御部
半導体メモリ
データ入出力インターフェース部
３０
２００
２１９
再生信号ｃ
（記録信号ｄ）

【図１０】


１５０
パーソナルコンピュータシステム
１４４
ＥＩＳＡバスコントローラ
ＥＩＳＡバス
１２６
サウンドブラスタボード
１２７
１２９
スピーカ
マイク
１２８
１１８
１４５
ＩＯアドレスライン
ＩＯデータライン
キーボードコントローラ
キーボード
１１９
ＩＤＥコントローラ
ＨＤＤ
１２１
情報再生装置
１２２
１４６
１２０
１１３
メモリアドレスライン
１１１
メインＣＰＵ
メインメモリ
１１２
メモリデータライン
１１５
１１４
ＬＣＤコントローラ
ＣＲＴディスプレイ
１１６
ビデオＲＡＭ
１１７
１２３
パラレルＩ／Ｆコントローラ
プリンタ
１２４
スキャナ
１２５
１３０
シリアルＩ／Ｆコントローラ
ＲＳ－２３２Ｃ信号ｅ
モデム
１３２
電話回線ｆ
１３１
１４３
ＰＣＩバスコントローラ
ＩＥＥＥ１３９４Ｉ／Ｆボード
ＩＥＥＥ１３９４信号ｇ
ＬＡＮ信号ｈ
ＰＣＩバス
１３３
ＬＡＮボード
１３９
音声符号化復号化ボード
ＭＰＥＧボード
サブピクチャーランレングス用ボード
専用ＤＳＰ
ＳＣＳＩボード
情報記録再生装置
１３６
１３４
１３５
１３７
１３８
１
ＭＴ
ＨＤＤ
１４２
１４１

【図１１】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６７５Ａ

(72)発明者　石沢　良之
神奈川県川崎市幸区柳町70番地　株式会社
東芝柳町工場内

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第４区分
【発行日】平成16年8月5日(2004.8.5)

【公開番号】特開平11-45507
【公開日】平成11年2月16日(1999.2.16)
【出願番号】特願平9-198638
【国際特許分類第７版】
Ｇ１１Ｂ　20/10
Ｇ０６Ｆ　12/14
Ｇ０９Ｃ　 1/00
Ｈ０４Ｌ　 9/08
Ｈ０４Ｌ　 9/32
【ＦＩ】
Ｇ１１Ｂ　20/10　　Ｄ
Ｇ０６Ｆ　12/14　　３２０Ｂ
Ｇ０９Ｃ　 1/00　　６６０Ｇ
Ｈ０４Ｌ　 9/00　　６０１Ａ
Ｈ０４Ｌ　 9/00　　６０１Ｅ
Ｈ０４Ｌ　 9/00　　６７５Ａ

【手続補正書】
【提出日】平成15年7月16日(2003.7.16)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報記録媒体から再生した情報の種類を判別する判別手段と、
この判別手段の判別結果に基づいて複数の認証相手の１つを認証相手と設定する設定手段と、
を具備したことを特徴とする情報再生装置。
【請求項２】
情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報再生装置以外の特定の認証相手に対して情報の伝送を行う通信手段と、
この通信手段を用いて上記認証相手に対して認証を行う認証手段と、
を具備したことを特徴とする情報再生装置。
【請求項３】
認証処理を行う認証処理制御部と認証処理の内容を記憶する認証情報記憶部とを具備し、
上記認証処理制御部による認証処理の履歴を上記認証情報記憶部に逐次記憶することにより、複数の認証相手との間の並行認識処理を可能とすることを特徴とする認証装置。
【請求項４】
複数の認証相手から個々に第１の暗号鍵を受け取る受け取り手段と、
複数の認証相手に対して個々の第２の暗号鍵を発行する発行手段と、
上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成する作成手段と、
複数の認相手に対して別々に上記各手段に対する処理の履歴を記憶する記憶手段と、

を具備したことを特徴とする認証装置。
【請求項５】
複数の認証相手から個々に第１の暗号鍵を受け取るステップと、
複数の認証相手に対して個々の第２の暗号鍵を発行するステップと、
上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成するステップとを有し、
複数の認証相手に対して別々に上記各ステップに対する処理の履歴を逐次記憶し、この記憶されている処理の履歴により、複数の認証処理を並行して実行することを特徴とする認証装置。
【請求項６】
少なくとも暗号鍵の発行とこの発行される暗号鍵に基づいた情報の暗号化と上記発行される暗号鍵に基づいた情報の復号化を行う認識装置において、
上記暗号鍵の発行、情報の暗号化、情報の復号化を行う際に用いるランダム信号を発生する発生手段を具備していることを特徴とする認証装置。
【請求項７】
認証相手からの第１の暗号鍵を受け取る受け取り手段と、
認証相手に対する第２の暗号鍵を発行する発行手段と、
上記認証相手から受け取った第１の暗号鍵と認証相手に対して発行した第２の暗号鍵を用いて認証相手との間で共通の第３の暗号鍵を作成する作成手段と、
情報を上記第３の暗号鍵を用いて暗号化する暗号化手段と、
暗号化されている情報を上記第３の暗号鍵を用いて復号化する復号化手段とを具備し、
上記作成手段、暗号化手段、復号化手段が１つの回路で構成されることを特徴とする認証装置。
【請求項８】
情報を再生する情報再生装置と、この情報再生装置により再生される情報を処理する情報処理回路と、上記情報再生装置と上記情報処理回路を制御するメインＣＰＵとからなる情報処理システムにおいて、
上記メインＣＰＵを介在せずに、上記情報再生装置と上記情報処理回路との間で相互認証を行うことを特徴とする情報処理システム。
【請求項９】
第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムにおいて、
上記第１の装置が、
識別用の情報を出力する第１の出力手段と、
この第１の出力手段に応答して上記第２の装置から供給される第１の暗号化キーに基づいて、あらかじめ記憶されている第２の暗号化キーを暗号化する第１の暗号化手段と、
上記識別用の情報に基づいて第３の暗号化キーを作成する第１の作成手段と、上記第１の暗号化手段により暗号化された第２の暗号化キーと、上記第１の作成手段により作成された第３の暗号化キーとを出力する第２の出力手段と、
この第２の出力手段に応答して上記第２の装置から供給される暗号化されている第４の暗号化キーを上記作成手段により作成された第３の暗号化キーを用いて復号化する第１の復号化手段と、
この第１の復号化手段により復号化された第４の暗号化キーと上記第２の暗号化キーとに基づいて共通鍵を生成する第１の生成手段と、
この第１の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第１の処理手段とからなり、
上記第２の装置が、
上記第１の装置から供給される上記識別用の情報に基づいて第１の暗号化キーを作成する第２の作成手段と、
この第２の作成手段により作成された第１の暗号化キーとを出力する第３の出力手段と、

この第３の出力手段に応答して上記第１の装置から供給される第３の暗号化キーに基づいて、あらかじめ記憶されている第４の暗号化キーを暗号化する第２の暗号化手段と、
この第２の暗号化手段により暗号化された第４の暗号化キーを出力する第４の出力手段と、
上記第３の出力手段に応答して上記第１の装置から供給される第２の暗号化キーを上記第２の作成手段により作成された第１の暗号化キーを用いて復号化する第２の復号化手段と、
この第２の復号化手段により復号化された第２の暗号化キーと上記第４の暗号化キーとに基づいて共通鍵を生成する第２の生成手段と、
この第２の生成手段により生成された共通鍵を用いて情報の符号化、復号化を第２の処理手段とからなる
ことを特徴とする情報処理システム。
【請求項１０】
第１の装置と複数の第２の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムにおいて、
上記第１の装置が、
ＡＧＩＤ、設定エリア情報、ストリームＩＤからなる識別用の情報を出力する第１の出力手段と、
時変情報に基づいて第１の暗号化キーを生成する第１の生成手段と、
上記第１の出力手段に応答して上記第２の装置から供給される暗号化されている第１のチャレンジキーを上記識別用の情報からなる合成キーに基づいて復号化する第１の復号化手段と、
この第１の復号化手段により復号化された第１のチャレンジキーに基づいて、上記第１の生成手段により生成される第１の暗号化キーを暗号化する第１の暗号化手段と、
時変情報に基づいて第２のチャレンジキーを生成する第２の生成手段と、
上記識別用の情報からなる合成キーに基づいて、上記第２の生成手段により生成される第２のチャレンジキーを暗号化する第２の暗号化手段と、
上記第１の暗号化手段により暗号化された第１の暗号化キーと、上記第２の暗号化手段により暗号化された第２のチャレンジキーとを出力する第２の出力手段と、
この第２の出力手段に応答して上記第２の装置から供給される暗号化されている第２の暗号化キーを上記第２の生成手段により生成された第２のチャレンジキーを用いて復号化する第２の復号化手段と、
この第２の復号化手段により復号化された第２の暗号化キーと上記第１の生成手段により生成される第１の暗号化キーとに基づいて共通鍵を生成する第３の生成手段と、
この第３の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第１の処理手段とからなり、
上記第２の装置が、
上記第１の装置から供給される上記識別用の情報に基づいて第１のチャレンジキーを生成する第４の生成手段と、
この第４の生成手段により生成された第１のチャレンジキーとを出力する第３の出力手段と、
この第３の出力手段に応答して上記第１の装置から供給される暗号化されている第２のチャレンジキーを、上記第１の装置から供給される上記識別用の情報からなる合成キーに基づいて、復号化する第３の復号化手段と、
時変情報に基づいて第２の暗号化キーを生成する第５の生成手段と、
上記第３の復号化手段により復号化された第２のチャレンジキーに基づいて、上記第５の生成手段により生成される第２の暗号化キーを暗号化する第３の暗号化手段と、
この第３の暗号化手段により暗号化された第２の暗号化キーを出力する第４の出力手段と、
上記第３の出力手段に応答して上記第１の装置から供給される暗号化されている第１の暗

号化キーを上記第４の生成手段により生成された第１のチャレンジキーを用いて復号化する第４の復号化手段と、
この第４の復号化手段により復号化された第１の暗号化キーと上記第５の生成手段により生成される第２の暗号化キーとに基づいて共通鍵を生成する第６の生成手段と、
この第６の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第２の処理手段とからなる
ことを特徴とする情報処理システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正の内容】
【００２２】
【課題を解決するための手段】
この発明の情報再生装置は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報記録媒体から再生した情報の種類を判別する判別手段と、この判別手段の判別結果に基づいて複数の認証相手の１つを認証相手と設定する設定手段からなる。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】削除
【補正の内容】